Global Information Assurance Certification Paper

Meeting FISMA Requirements for Systems
Constructing a System Security Plan

SANS Security Essentials
GSEC – Practical Assignment, v1.4b, Option 1

By Daniel J. Nagy
March 24th, 2004

Abstract

Over the last decade the public sector has adopted a much more open approach to using information systems. With the influx of an increased variety and quantity of information systems, stringent laws and regulations have come into being. With the December 2002 Federal Information Security Management Act (FISMA), Federal agencies are now accountable in full for the security of their systems.

Many agencies, including the United States Department of State, require as part of a formal Certification and Accreditation process (C&A) that a System Security Plan (SSP) be created for every application and support system in development or production. This paper addresses the required information and structure for constructing a System Security Plan to meet C&A requirements.

Introduction

In December of 2002, President George W. Bush signed Public Law 107.347 (the "E-Government Act") that contains the Federal Information Security Management Act (FISMA[1]). Set to replace the Government Information Security Reform Act (GISRA[2]) of 2000, FISMA requires government agencies to perform annual Information Technology (IT) security reviews, reporting and remediation planning.

At the time of this writing, the Internet connects over 170,000,000 devices and continues to expand at a rapid pace. At any given point in time, there are millions of connected devices that are vulnerable to worms, viruses or denial of service attacks. Malicious organizations and individuals alike can take advantage of these vulnerable machines in order to steal information, modify existing data or harness them together to create large-scale attacks.

The majority of reported attacks are fully automated through the use of readily available tools. Due to the proliferation of powerful, low-cost computers, these attacks are inexpensive to mount, allowing any individual or organization the ability to sortie. With available tools that require little to no actual system or security knowledge, an attacker can be from any educational, ethnic and economic background. "The sophistication of the attack is growing, but the sophistication of the attacker is not.[3]"

The public sector has become increasingly dependent on the Internet, using it for mission critical applications, communications and intelligence

[1] http://csrc.nist.gov/policies/FISMA-final.pdf
[2] http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106_cong_bills&docid=f:h5408ih.txt
[3] http://csrc.nist.gov/sec-cert/PPT/Workshop-1.ppt

gathering. Short interruptions in service can cause significant economic loss, possibly jeopardizing lives.

In the years ahead the Federal government's reliance on the Internet will continue to. The healthy functioning of the Internet will be essential to national security. "The federal government has spent billions of dollars supporting the planning, development, and operation of state systems[4]" This time and money provides insights into effective strategies for not only improving public sector security, but are also providing valuable models for the private sector.

FISMA is now the key driver with which the Federal government will approach the challenge of improving its IT security for the future. FISMA is based on real-world lessons learned and identified through countless years of audits and assessments. FISMA was authored with the assistance of the professional audit community. Many of the provisions of FISMA have roots in IT audit methodologies that apply to both commercial and government organizations.

Many steps must be taken to create a security program and timeline to meet FISMA standards for major applications and general support systems. One of the most critical sections of this process is the development of a System Security Plan (SSP). This document provides an overview of the security requirements needed for the system, descriptions of controls that are planned, in-place and the responsibilities and behavior required by individuals managing and using the system. The SSP document provides four crucial categories of information: system identification, management controls, operational controls and technical controls.

1. System Identification

This category provides an overview of the basic elements comprising the system. Many of the sections included below are terse versions of information found in later sections of the document.

Section 1.1 "System/Site Name"

The information system must be given a unique identifier to distinguish it from similar systems. Due to the sheer number of information systems currently in use and slated to be implemented, this unique identifier is crucial for future referencing. For example, in the development of an SSP for a Major Application (MA), one if not more General Support Systems (GSS) are usually referenced. Since many systems can be similar in nature and functions, these unique identifiers provide security auditors a clear understanding of the systems involved.

[4] http://www.gao.gov/new.items/d02347t.pdf

Besides giving a clear meaning, the unique identifier is also required by the Information Technology Management Reform Act of 1996[5] as it is an integral piece in IT investment models and analysis. The identifier should follow the system for the remainder of its life cycle to allow tracking the completion of security controls.

Section 1.2 "Responsible Organization"

All systems falling within the scope of an SSP require that current contact information be provided. Under FISMA, all major applications and general support systems are required to have a singular organizational point of contact, which takes responsibility for all facets of the system. Generally speaking, this contact will be the branch or division chief of the organization responsible for the development of the system.

Section 1.3 "Informational Contacts"

Informational contacts are defined as individuals who control individual roles relating to the system. Some common roles would include contingency planning coordinator, the System Owner (SO), Information System Security Office (ISSO), network engineers, system administrators, and other related roles.

Section 1.4 "Assignment of Security Responsibility"

An individual assigned to serve as the ISSO will be ultimately responsible for the security of the entire MA or GSS. A backup or alternate ISSO should also be provided. Both the ISSO and alternate should be aware and fluent in all controls comprising the system.

Section 1.5 "System Operational Status"

The system operational status should be assigned to one of the following as defined in NIST SP 800-64[6]:

- Initiation Phase
- Development / Acquisition Phase
- Implementation Phase
- Operation/Maintenance Phase
- Disposal Phase

These are fully explained in section 2.5 "Planning for Security in the Life Cycle". The inclusion of the status in this section is for reference purposes.

[5] http://govinfo.library.unt.edu/npr/library/misc/itref.html
[6] http://csrc.nist.gov/publications/nistpubs/800-64/NIST-SP800-64.pdf

Section 1.6 “General Description/Purpose”

This section requires a brief summary of the purpose and goals of the system. The highest security level of information processed within the system should be listed along with any GSS systems the system relies upon. A list of organizations allowed to access the system should be listed, along with any specific criteria individual organizations must meet.

Section 1.6.1 “System Category”

The system the SSP covers must fall into one of two categories: Major Application (MA) or General Support System (GSS). A GSS can be defined as a system upon which other systems rely, such as a network. A Major Application is a specific piece of software that provides services over a GSS.

Commercial Off The Shelf (COTS) software such as word processors, email clients and other general purpose software are generally not considered to be MA’s and are covered by the SSP for the GSS on which they are installed.

Section 1.6.2 “Multiple Similar Systems”

If any similar systems exist within the organization, these are usually declared along with the differences between them. Physical location, responsible organizations or classification levels are examples of differences.

Section 1.7 “System Environment”

Brief summaries of the technical aspects of the system are listed, including any items that raise security concerns. If the system is connected to the Internet, publicly accessible, in a dangerous area, etc. these should be noted along with any documentation pertaining to the listed items.

Along with this, the physical location of the system should be declared, what hardware and operating system are used and a brief overview of any security software implemented such as firewalls and anti-virus software.

Section 1.7.1 “Components”

A more in-depth explanation of the software, hardware and communication lines used by the system should be listed here. Any security controls in place to protect the system and information within should be explained. Only security controls currently in-place should be listed.

Section 1.7.2 “System/IT Boundaries”

System boundaries list all processing, communication, storage and related resources, their physical locations and an outline of any networks connected to these systems. A lengthier explanation follows, describing details on the interconnection of systems including reciprocal connections, Internet access and any other miscellaneous boundary overlap.

Section 1.7.3 “Hardware”

This section should categorize all systems contained within the system boundary. Every different type of server (e.g., web, mail, database) should be accounted for. For each type, the operating system and software used should be itemized, along with the corresponding documentation for both the operating system and the specific service software.

Section 1.8 “System Interconnection/Information Sharing”

Since many Federal agencies perform interconnected duties, systems may need to interconnect to share information. If the measures in place to protect the interconnection are not adequately secure, a compromise of systems on both ends can occur.

Depending on the organization authoring the SSP, interconnected systems may require a written agreement (often known as a Memorandum of Understanding) prior to the systems communicating. The documentation must provide set rules of behavior to be followed by both systems. The rules of behavior for the system are detailed in section 2.3 “Rules of Behavior”.

Section 1.9 “Sensitivity of Information Handled”

This section provides information dealing with the sensitivity and relative importance of any information processed, transmitted or stored within the system.

Section 1.9.1 “Laws, Regulations and Policies Affecting the System”

Laws and regulations pertaining to the system should be listed here. This must include all references to materials pertaining to information sharing and classification such as the Freedom of Information Act (FOIA[7]) and the Privacy Act of 1974 (5 U.S.C. 552a[8]), system security documentation such as NIST FIPS[9]

[7] http://www.usdoj.gov/04foia/referenceguidemay99.htm#intro
[8] http://www.usdoj.gov/foia/privstat.htm
[9] http://csrc.nist.gov/publications/fips/

manuals. These referenced documents provide a baseline for auditors when dealing with systems.

Section 1.9.2 "General Description of Sensitivity"

A general description of the level of information security is then presented. This text defines the maximum level of secrecy applied to the information processed within the system and the impact rating the disclosure of this information would cause. Under the new FISMA standards, government agencies assess the potential impact using the categories of confidentiality, integrity and availability (commonly known as the CIA triad). FISMA defines the CIA triad as follows:

- Confidentiality
  "Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…" [44 U.S.C., Sec. 3542]

- Integrity
  "Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity…" [44 U.S.C., Sec. 3542]

- Availability
  "Ensuring timely and reliable access to and use of information…" [44 U.S.C., SEC. 3542]

Section 1.10 "System SCL Level"

This end result, known as a Security Categorization (SC) is comprised of evaluating the impact level of the listed categories. FISMA states that for any applicable information or information systems, a level of potential impact must be assigned to the previously listed categories. Each impact level is assigned a score between one and three. FISMA defines these levels as the following:

- Low
  "The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals." This status is scored as 1 on the SC.

- Medium
  "The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals." This status is scored as 2 on the SC.

- High
  "The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals." This status is scored as 3 on the SC.

The SC must also assign values to the criticality and complexity of the system. The criticality of the system is marked as one of the following:

- Mission Critical
  Mission critical status should be selected if the system provides core business functions that would cause an immediate business failure. This status is denoted as a score of 3 on the SC.

- Mission Important
  Mission important status should be chosen if the system provides a secondary approach to the processing of critical data. In the event of system failure, the negative impact would occur over a span of time. This status is denoted as a score of 2 on the SC.

- Mission Supportive
  Mission supportive status is chosen when the loss of the system would only cause a minor inconvenience. This status is denoted as a score of 1 on the SC.

When assigning criticality, encompass the entire system. Even if safeguards are in place such as backup servers and redundant connectivity, consider only the loss of the system as a whole.

The complexity of the system is measured as the amount of instances (locations) and the number of interfaces (interdependencies). Instances are also scored on a 3-point scale where worldwide/department wide is a score of 3, bureau wide is a score of 2, and local to the office is a score of 1. The amount of interfaces determines the score given. Four interfaces or greater is a score of 3, 2 or 3 interfaces is a score of 2 and less than 2 is a score of 1.

Once all the scores for each category are assessed, the total SCL must be calculated. If the total is 13 or greater, the SCL score is 3. If the score is between 10 and 12, the SCL score is 2. If the score is between 7 and 9, the SCL score is 1. Systems with a SCL total less than 7 are considered to have a 0 score and are not considered to be a major application. Any systems scoring a 0 score do not currently require completion of a SSP.

	CRITICALITY	CONFIDENTIALITY	INTEGRITY	AVAILABILITY	INSTANCES	INTERFACES	TOTAL		SCL SCORE
VALUE	3	3	3	2	1	1	13		3

Figure 1.1: Example SCL

2. Management Controls

This section describes "the management control measures (in place or planned) that are intended to meet the protection requirements of the major application or general support system. Management controls focus on the management of the computer security system and the management of risk for a system. The types of control measures shall be consistent with the need for protection of the major application or general support system.[10]"

Section 2.1 "Risk Assessment and Management"

Risk Assessment (RA) details the results of both a technical and non-technical RA. Risk Assessment can be defined as "The process of identifying the risks to automated information resources and information, as part of a risk-based approach used to determine adequate security for a system by analyzing the threats and vulnerabilities and selecting appropriate cost-effective controls to achieve and maintain an acceptable level of risk.[11]" Any planned or completed risk assessments are listed, along with any information pertaining to internal system reviews by the IT security staff identifying any areas of concern.

Section 2.2 "Review of Security Controls"

All Federal agencies require annual auditing of security controls via self-assessments or independent review. The schedule required by the responsible organization should be listed along with all findings of any previous reviews. If any major deficiencies have been recorded, indicate what steps have been taken along with a timeline to fixing the problem.

---

[10] http://www.it.kmitl.ac.th/chanboon/cs/SP800-18.pdf

[11] US Department of State, Office of Information Assurance "System Security Plan Quick Guide" December 2003

Section 2.3 "Other System Evaluation Approaches"

Non-formal reviews can take place in the interim between annual audits. Since technology changes regularly, the use of vulnerability assessment tools (port scanners, patch management tools, etc.) can be useful in assessing weaknesses in security controls. List any such activities along with the date and findings in this section.

Section 2.4 "Rules of Behavior"

"A set of rules of behavior must be established for each system. The security required by the rules is only as stringent as necessary to provide adequate security for the system and the information it contains. The acceptable level of risk should form the basis for determining the rules.[12]" They should cover such matters as work at home, dial-in access, connection to the Internet, use of copyrighted works, unofficial use of government equipment, the assignment and limitation of system privileges, and individual accountability. Any user requesting access should be provided with a copy of the document(s) describing these rules prior to being authorized to access the resource. A common method is to hold a security briefing during which the rules are explained and the user is required to sign an acknowledgement form. A copy of this document should be included within the SSP as an appendix.

Section 2.5 "Planning for Security in the Life Cycle"

As the SSP is a new process, we may have to apply it to preexisting information systems not just new ones. System owners must describe where within the system development life cycle the system lies. FISMA states the following as being required phases to account for:

- Initiation Phase
  During the initiation phase, the need for a system is expressed and the purpose of the system is outlined. An assessment of the sensitivity of the information to be processed on the system should be conducted and be expressed here as well as in the Security Categorization from the preceding section.

- Development / Acquisition Phase
  During this phase, the system is either developed or purchased as a commercial off-the-shelf (COTS) product. System planners should fully define the technical requirements of the system to be followed by the security staff declaring the required controls to meet security criteria. These requirements

[12] http://www.it.kmitl.ac.th/chanboon/cs/SP800-18.pdf

include access controls, background investigations, security briefings, training and other operational practices.

- Implementation Phase
  In this phase, the finalized system's security requirements will be enabled, tested and installed. Prior to production status, a design review and test should be performed to ensure confidence in the security specifications. Any new security requirements added at this point should be tested for the previously stated reasons and also to ensure that the newer requirement does not interfere with previously implemented controls. All these reviews and tests should be fully documented and either appended to the SSP or made available to the auditors.

- Operation/Maintenance Phase
  During this phase, the system has been implemented and is in production status. Most operations during this phase are comprised of the addition of hardware and software in order to maintain stability and security. Most documentation accompanying this phase included reoccurring activities such as backup procedures, holding security briefings, user and system administration and keeping software patched.

  Periodic audits should occur to guarantee that the system is being used in the proper manner. This may involve auditing or monitoring of actions performed by users, administrators and other security controls. Results of these audits should be compared to the current security controls to ensure that the controls in-place are performing correctly.

- Disposal Phase
  The disposal phase of information systems deals with the removal and destruction of information, hardware and software pertaining to the system. Often an overlooked section of the life cycle, proper controls for the eradication of materials is essential to preserving security.

  Although many systems under the disposal phase are being replaced by new systems, a system may merely come into a state of disuse. Information contained within systems being upgraded is often rolled in as legacy data, but when a system is removed in entirety, steps must be taken to ensure the archival of information is done in a secure manner. The information should be protected by using cryptographic keys and stored in a safe, accessible location, such as a pre-defined data vault. Many Federal organizations have defined offices for retaining archived information.

  Media previously related to the systems in question should be properly sanitized dependant on the level of security required. The ISSO must decide if merely clearing the information (media formatting) is sufficient or if purging

the media is required. The three common methods of purging media are overwriting, degaussing and destruction.

During the life cycle process, a given information system can be in more than one phase. Large systems may be in a development phase at the same time as an operation maintenance phase. Each phase the system is currently considered to be in should be properly documented.

Section 2.6 "Authorized Processing"

The last entry under management controls defines authorized processing. Authorized processing is merely authorized permission to let the information system process information within its security bounds. Different Federal organizations have different processes in order to reach authorized processing status.

The primary reason for authorized processing is to provide a point of contact that approves the current managerial, operational and technical controls before the system may fully function. This person must ensure that all federal laws, regulations and standards are met, a formal risk assessment has been conducted, the rules of behavior are in place, all safeguards are operating as intended and that a robust contingency plan has been put in place. While much of this would seem to fall into the realm of duties occupied by an ISSO, authorization to process must be granted by either a representative of the organization supported by the system or a Designated Approving/Accreditation Authority (DAA) such as a CIO.

3. Operational Controls

Operational controls deal with the most important part of security, which are the day-to-day operations pertaining to the system. Most operational controls are implemented and executed by people as opposed to the system. A good way to view operational controls is as the security controls in place to protect and maintain the environment in which the system exists. Often, too much emphasis in the information security domain is placed in technical controls as opposed to the physical realm.

The SSP document requires that operational controls be labeled using the Security Control Measure Status (SCMS). The SCMS rating is evaluated using the following scale:

- In Place
  Operational controls marked in place are operational and deemed to be effective for the classification level of the information processed.

- Planned
  Planned controls are control measures that are either new to the system or are in the process of being upgraded.

- In Place and Planned
  Controls falling under this status are a combination of operational controls and controls not yet implemented.

- Not Applicable
  This describes any control that either does not apply to the system or is not deemed to be cost-effective.

Section 3.1 "Personnel Security"

The greatest security risk to any information system is the actions of individuals, both intentional and unintentional. Personnel security is essential to minimizing the possible effects that authorized personnel can have on the system.

This section should contain information pertaining to required background investigations appropriate for the sensitivity level of the information processed on the system. Depending on the system, a different clearance level may be required for application users, database administrators (DBAs), application developers and other technical positions.

Access to the data center(s) housing the system must also be defined. Since the data center(s) may contain systems of more than one sensitivity level, the data center manager must declare restrictions on what areas inside of the data center(s) are restricted. Non-technology based positions such as custodians and maintenance workers must also be accounted for. It is assumed that they will be under full visual observation while accessing sensitive areas.

Section 3.2 "Physical and Environmental Protection"

This section addresses controls in place at the actual location housing the system. This includes both physical/environmental controls in-place and planned. A few examples include smart cards, cipher locks, raised flooring, independent wiring/HVAC systems and CCTV cameras. The SSP requires that seven areas be identified:

- Access Controls
  The writer must address all physical entrances and exits to the areas housing the system. This also includes any accessible cabling, public utilities supporting the system and any backup media storage such as a data vault. The effectiveness of these controls must be evaluated for different periods of activity, such as during and outside of business hours.

- Fire Safety Factors
  While the protection of the computing resources is critical, it in no way overrides any risk to human lives. This section should address the behavior of controls in the event of a fire such as the automatic shutdown of any electronic door locks and emergency lights.

- Failure of Supporting Utilities
  The areas containing the system are expected to be environmentally stable. Failure of any utilities such as power, HVAC and water can cause major damage to hardware and cause availability issues. Any systems in place to minimize problems in the event of an outage such as uninterruptible power supplies (UPS) and generators should be noted along with their maximum operational time.

- Structural Collapse
  The buildings housing resources may be subjected to a load greater than they can support. This includes damage from earthquakes, explosions, fire and snow accumulation. While this is certainly not preventable, any existing structural reinforcements should be addressed along with a reference to any disaster recovery plans.

- Plumbing Leaks
  Since water is the natural enemy of electronic devices, the location of any water pipes should be documented along with steps to reducing risk such as moving hardware, moving pipes and identifying shutoff valves.

- Interception of Data
  Depending on the sensitivity of information processed within the system, the risk of interception will vary. Direct observation entails line of sight viewing by unauthorized parties, such as viewing data from a remote location such as an adjacent building. Interception of data transmission can result from an ethernet splice, intercepting wireless transmissions or trojan programs. Electromagnetic interception deals with the monitoring of minute transmissions for electronic equipment and reproducing these signals into meaningful information.

- Mobile and Portable Systems
  As a growing number of systems provide computing resources to users in the field, portable computers must be taken into account. If the system is located within the confines of a vehicle, it inherits the same risks as the vehicle. All computers should be securely stored when not in use and sensitive data encrypted to an appropriate measure.

Section 3.3 “Production Input/Output Controls”

This section is meant to detail all the activities that support the operation of the system. Some examples of items that fall into this category are user support services, appropriate labeling and handling of printed material and backup media and the destruction of said media. Poor handling of media can lead to a serious breach of security whether it be from lack of proper inventory control or not properly destroying media via shredding, degaussing and other means.

Section 3.4 “Contingency Planning”

In the event that a system should be destroyed or temporarily unavailable, an organization must be prepared. Contingency plans, business interruption plans and continuity of operation plans need to be accounted for, along with any documentation available for all GSS systems.

All contingency plans must be regularly tested in preparation for catastrophic events. If a regular schedule for testing plans is available, it should be included. All plans must also be made readily available to the appropriate staff for use in emergency situations.

Finally, all backup and restoration procedures of systems should be fully documented. This includes not only the backup schedule but also the location of stored backups, how many months of backups are kept, the type of backup procedures in use (differential, full, etc.) and what exact data is being archived.

Section 3.5 “Maintenance Controls”

The primary focus in this section is the change management/version control of the application(s) used by the system. Ensuring that only legal, approved software is contained within the system prevents problems regarding software piracy and licensing issues.

Firstly, all software used by the system should be identified as being either bought commercial software or in-house developed software. All software developed in-house should be marked as being built by government workers or contractual workers. If the software was created by another Federal agency, ownership of the product should be noted. In the case of commercial software, proof of purchase and/or licenses should be provided.

If the software was developed in-house, all procedures pertaining to updates, testing and deployment must be properly documented. All formal testing results should be made available upon request. In the case of emergency fixes, a brief summary should be provided explaining the expedited patching process.

Operating system and related software must also be accounted for. The primary focus should be on the regular maintenance and purchasing agreements for the software as the configuration and lockdown procedures have been documented in previous sections.

Finally, if warranted, procedures for checking for the existence of illegal software on both production systems and users desktops should be referenced. If the authoring organization has any regulations and penalties for use of illegal software, they should be specified either in this section or as an appendix.

Section 3.5.1 "Hardware Maintenance Controls"

All personnel responsible for the service and maintenance of systems and related GSS systems must have a clearance reflection the sensitivity of information processed on the system. Any regulations regarding service contracts should be declared, along with the processes of sending damaged systems off-site.

Section 3.6 "Data Integrity/Validation Controls"

Data integrity controls are used to prevent the intentional or accidental modification or deletion of data. These controls are commonly represented by test results and evaluations of the security controls in place. Some examples of integrity controls are the output from password crackers/checkers, intrusion detection systems (IDS) and any penetration testing done to the system in its production environment.

Section 3.6.1 "Malicious Programs"

This section should describe processes used in guaranteeing that malicious programs such as trojan horses and spyware will not be installed either accidentally or maliciously. A common program used to monitor core system files is Tripwire [http://tripwire.com/]. Tripwire provides change control monitoring by uniquely marking files with an MD5 sum and comparing it on regular intervals.

Section 3.6.2 "Virus Protection"

Almost every government agency requires the use of anti-virus software. Organizations must document the software used, processes involved in updating virus signature files and what media is to be monitored in real time. Any planned measures should also be documented, such as an upgrade in version of the software used.

Along with the practical use of the software, procedures pertaining to the destruction or removal of systems on which the virus cannot be eradicated should be listed. The ISSO and system administrators should make every effort in pinpointing the origin of the virus and send the information to the appropriate organization for inspection.

Section 3.6.3 "Message Authentication"
Section 3.6.4 "Integrity Verification"
Section 3.6.5 "Reconciliation"

The above sections all deal with any controls in place to assure the confidentiality and integrity of data sent to the system by users. Any measures used to ensure security (such as IPSec, VPN and other encryption technologies) should be explained.

Section 3.6.6 "Digital Signature"

As many systems are now fully replacing what used to be lengthy human processes, the use of digital signatures are rapidly replacing paper and pen signatures. As digital signatures can now be used as a standard of proof under the law, it is important to fully document any encryption algorithms and software used to implement digital signatures.

Section 3.6.7 "Intrusion Detection and Monitoring"

If any intrusion detection systems are used either on the server or the GSS supporting the system, they should be documented here. Explanations of monitoring and incident response may also be added.

Section 3.7 "Documentation"

Documentation provides an explanation as to how hardware and software are to be used and provides security and operational baselines. Although many of the items relating to this have probably already been referenced, re-list all documentation (policies, standards, etc.) pertaining to the system and any GSS that are used. Whenever possible, provide either a hyperlink or a physical location where the document can be provided.

Section 3.8 "Security Awareness and Training"

Before access to resources is provided to a user, the user must complete an initial security awareness class. The purpose of this class is to explain the acceptable rules of behavior when using the system and how sensitive materials should be handled. Regular refresher briefings are required and can be used to inform users of new rules and regulations pertaining to systems.

This section should describe the above items, along with a formal schedule. Any awareness items (books, posters, etc.) should be documented along with training materials used in the class.

Section 3.9 “Incident Response Capability”

A security incident can be defined as a successful or attempted breach of security controls. Due to the increasing amount of attacks that have occurred over the past few years, documentation detailing the identification and appropriate response activities should be prepared for every system.

Some of the more common issues should also be addressed, such as a formal process for reporting incidents. If the organization has a Computer Incident Response Team (CIRT) any available documentation may be referenced as to how incidents are handled.

4. Technical Controls

Technical controls are used to add restrictions on access to systems and to protect information. This section primarily deals with using automated security controls to preserve CIA.

Section 4.1 “Identification and Authentication”

Identification is defined as the means of providing an identity to the system. Although the most common form of identification in computer systems is the username, other means of identification such as a smartcard are in use. If the system uses usernames as the primary means of identification, a description of the minimum and maximum amount of characters, non-allowed characters and any other formatting rules should be defined.

Authentication is defined as the means of proving the validity of the identification given to the system. As the username is the most common form of identification, a password is the most common form of authentication. As computers become less expensive, newer forms of authentication are replacing the password, including biometrics, smart cards and other tokens.

All controls in place that handle identification and authentication should be documented and explained. If passwords are used for authentication, the following sections should be completed in full.

Section 4.1.1. "Password Length"

A minimum and maximum character boundary should be set for all passwords. Most modern systems require the password be greater than 7 characters.

Section 4.1.2 "Password Composition"

Here the form of the password should be defined. List any characters that are not permitted, along with any formatting issues (e.g., can not begin with a digit). Many systems now require that a password be composed of characters, numbers and non-alphanumeric characters (punctuation).

Section 4.1.3 "Password Maintenance"

This section defines the entire lifecycle of a password. Items such as the lifetime of the password, procedures in the event of losing or revealing a password, handling of failed logon attempts and how the passwords are stored within the system should be fully documented and in compliance with any regulations required by the organization.

Section 4.2 "Logical Access Controls"

Logical access controls are automated controls that limit access to system resources by predetermined rules. These rules can pertain to both users of the system and processes within the system. Since the primary goal of logical access controls is to preserve confidentiality, integrity and availability there are far too many considerations to list in entirety. As a brief starting point, the following should be considered:

- Default roles/groups that are provided to users and processes for promoting and demoting user privileges
- Access Control Lists (ACLs)
- Availability of system resources
- Removal/deactivation of accounts no longer in use
- Firewalls, intrusion detection systems and other tools
- Use of trusted domains
- Restrictions based on dates or time
- BIOS authentication
- File permissions
- Encryption of files or connections
- Dial-up access

Section 4.3 "Public Access Controls"

Any systems that are available for public use must take special precautions. At no time should any sensitive systems provide information/interconnection to publicly available systems. If the system must provide access to the public, any controls in-place should be defined.

Due to the probability for attack on a public system, programs and information available should be made as secure as possible. All data should be ensured to be virus-free and read from a read-only media such as a CD-ROM if possible.

Section 4.4 "Audit Trails"

Audit trails are automated system messages informing system administrators of pre-defined activities by users. Audit trails provide an excellent resource in hunting down both system issues and security incidents. All facets of auditing should be accounted for, such as what activities are monitored, what information is recorded and what personnel have access to the logs.

Another type of audit trail, keystroke monitoring, is also something that should be documented if in use. As of the date of this writing, there is still no formal document declaring the legality of this practice. "If the courts were to decide that such monitoring is improper, it would potentially give rise to both criminal and civil liability for system administrators. Therefore, absent clear guidance from the courts, we believe it is advisable for system administrators who will be engaged in such monitoring to give notice to those who would be subject to monitoring that, by using the system, they are expressly consenting to such monitoring. Since it is important that unauthorized intruders be given notice, some form of banner notice at the time of signing on to the system is required. Simply providing written notice in advance to, only authorized users will not be sufficient to place outside hackers on notice.[13]"

Section 4.5 "Compensating Controls "

Finally, any other controls not falling into any of the previous sections should be listed. This includes controls that are implemented on GSS systems that the system relies upon. If any items fall under this category, the unique identifier of the system should be referenced, along with any supporting documentation.

Conclusion

The System Security Plan was created in response to FISMA's requirement for security accountability for information systems. The SSP addresses this requirement by providing a broad overview of security controls and documentation for information systems meeting high-security thresholds.

[13] http://doe-is.llnl.gov/Orders/dojkeymn.pdf

With the field of technology consistently changing, the SSP must be treated as a living document, living beyond the completion of the C&A process. In addition to use within the government, private sector industries can use the SSP documentation as a framework for creating their own processes.

The System Security Plan is an excellent standard that will prove to be a valuable tool for both the public and private sectors to use in building secure information systems.

References

"Federal Information Security Management Act of 2002", 12/2002
URL: http://csrc.nist.gov/policies/FISMA-final.pdf (3/10/2004)

"Government Information Security Reform Act", 9/6/2000
URL: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106_cong_bills&docid=f:h5408ih.txt (3/8/2004)

Ross, Dr. Ron. "FISMA Implementation Project: Protecting the Nation's Critical Information Infrastructure", 2/2/2001
URL: http://csrc.nist.gov/sec-cert/PPT/Workshop-1.ppt (2/19/2004)

McClure, David L. "Federal Approval and Funding Processes for States' Information Systems", 7/9/2002
URL: http://www.gao.gov/new.items/d02347t.pdf (3/2004)

"Information Technology Management Reform Act of 1996 (Summary)", 8/8/1996
URL: http://govinfo.library.unt.edu/npr/library/misc/itref.html (3/12/2004)

Grance, Tim; Hash, Joan; Stevens, Marc. "Security Considerations in the Information System Development Life Cycle", 9/2003
URL: http://csrc.nist.gov/publications/nistpubs/800-64/NIST-SP800-64.pdf (3/12/2004)

U.S. Department of Justice, "Freedom of Information Act Reference Guide", 11/2003
URL: http://www.usdoj.gov/04foia/referenceguidemay99.htm#intro (2/24/2004)

U.S. Department of Justice, "The Privacy Act of 1974", 6/1975
URL: http://www.usdoj.gov/foia/privstat.htm (3/2004)

Mueller, Robert S. "Department of Justice Letter on Keystroke Monitoring and Login Banners", 10/7/2002
URL: http://doe-is.llnl.gov/Orders/dojkeymn.pdf (3/9/2004)

Krutz, Ronald L.; Vines, Russell Dean. "The CISSP Prep Guide" Reading: Wiley Publishing Inc., 2003

Swanson, Marianne. "NIST Special Publication 800-18 Guide for Developing Security Plans for Information Technology Systems", 12/1998
URL: http://www.it.kmitl.ac.th/chanboon/cs/SP800-18.pdf (3/30/2004)