Global Information Assurance Certification Paper

The Value of Documentation: A Useful System Security Plan Template
Falan Memmott
April 21, 2001

Introduction

This paper is intended for those who may be new to the information security arena and who have been tasked short order with assembling a system security plan for a civilian agency Security Certification and Accreditation Package. A Security Certification and Accreditation Package requires several documents and is not limited to but may include these: Risk Assessment, Risk Mitigation Plan, System Security Plan, Certification Test Plan, Certification Test Report.

I used NIST Special Publication 800-18 as a guide for this paper about the value of system documentation and systems security plans. I have chosen to provide additional insight to the guide, and have built a template as a practical extension of the materials contained in 800-18. The basic purpose of this paper is to address the value of system documentation and it provides a System Security Plan (SSP) template that can be put to immediate use in the field.

Why Documentation?

One aspect of successfully managing an IT system is actively protecting it. In order to actively protect a system, you have to know what it is, what it does, what its weaknesses are, what potential threats to it exist, and what has or is being done to mitigate the risks to your data and system (DOJ).

Organizations that choose to passively protect their systems can lose vital institutional knowledge when something as simple as one mere employee is injured, retires, or follows a better opportunity. Yet how much more they lose when an employee willfully destroys data on their way out the door, or when an intruder alters access logs and creates hidden accounts. These examples illustrate what can come from what is essentially system negligence. Yet, all of these attacks on a system's availability, integrity, and confidentiality could have been addressed in a preventative manner through the results that come from having gone through the process of completing thorough system documentation.

Are systems really neglected? Funny you should ask. One of the most common but tragic efforts I have seen for attempting to get out of doing system documentation is the almost existential notion that, "if my data isn't sensitive, then it doesn't need protection, right?" Of course, people often take it a step further, and those in the Federal sector who do so may suddenly find themselves defending their existence to their Inspector General. Why people don't consider the consequences of stating that their system has no data of value on it puzzles

information assurance professionals to this day. The important point here is not to do it--or you may find yourself trying to prove that your organizational role is valid and that you really do need your IT budget. Do people really do this? Ask around. You'll be surprised.

OK. So, what does every manager really want? To be recognized, promoted, or build an empire of course. How can a manager arrive at these goals if they don't have the tools they need to make effective decisions? There is no legitimate means. This is because effective decisions cannot be made if what a system is, and what it does, etc, is not known.

Commonly, managers "have not instituted procedures for ensuring that risks are fully understood and that controls implemented to mitigate risks are effective" (GAO). Therefore, protection should be determined by evaluating the sensitivity and criticality of the information processed, the relationship of the system to the organization's mission, and the economic value of the system's components, among other factors.

At this point some may try to dismiss documenting system security since risk must be accepted as a part of doing business. While it is true that a decision must be made to proceed with risk acceptance or risk mitigation, all systems deserve risk-effective decisions to be made, and this can only be accomplished by having key information about the system available to the decision maker.

Another hazard of managers not clearly understanding their systems is that they will rely on technologists for advice. Being a technologist myself, I can admit that sometimes it is easier to take technology in search of a mission and to let technology dictate a system's requirements, rather than to build in security from the beginning. Besides, who has time for documentation when you get new "toys" to work with and "work" is sending you subliminal messages to leave that boring paperwork stuff alone.

Fortunately, times are changing with the advent of serious e-commerce, but it is still a rare thing for technologists in general to be rewarded for properly applying security to their systems. After all, we're rewarded for how transparently everything operates, how fast processors can churn, and for how quick we can get that next software release out, not for bogging the system down by adding encryption etc., or for filling out forms on the status of your systems. For all of these reasons, it is clear that efforts should be made to thoroughly document a system's security.

Since security is historically, outside of the Department of Defense and financial industries, an afterthought, it is not uncommon that security requirements will come down through administrative channels in such a surprising fashion that all to often they leave bewildered information technologists or project managers wondering what to do.

So What Is A System Security Plan Anyway?

Best practices dictate that one of the best ways to document the protection afforded the system by managerial, operational, technical, and other means is by creating a system security plan. This is because a well-done SSP provides a concise location (OMB) of documented system requirements that can be readily utilized from the initial phases of a system's development through its disposal.

SSPs are of particular value because they address so many security-related facets of a system. In short, the material in an SSP will help in protecting the confidentiality, integrity, and availability of the system it is for because it documents the system's basic security requirements, the controls in place, planned controls, the responsibilities of system users, and expected user behavior (Swanson, 2). These five areas are key areas to document.

Documenting the five areas above provides a very useful concentration of security information—one that can be used throughout any systems development life cycle phase. The security requirements show developers, managers, and auditors alike, what the system should be allowed to do or not do. Documenting the controls in place, or the planned controls in instances of system development or remediation, identifies specifics about a system's security. Putting the responsibilities of system users in writing is vital since you can create a user policy / announcement that users have to sign that they have read them. By using this method as an opportunity to inform users about their security responsibilities, you can also increase their awareness of information security, as well as provide your organization recourse for user misbehavior.

Security Plan Template Overview

I have created APPENDIX A below as a guide to drafting a system security plan for new or existing general support systems. As you may be aware, NIST classifies systems as either "systems," "major applications" or "general support systems." Only major applications and general support systems are required to have system security plans because generic systems are likely to be included under the umbrella of one of the former.

When looking for detailed solutions, the NIST Special Publication 800-18 does an excellent job of describing a framework for a system security plan and should be referenced http://csrc.nist.gov/publications/nistpubs/index.html/ (NIST).

I have chosen to use an adapted fill-in-the-blank approach in order to simplify the process of adequately documenting a system via a SSP for the anxious information technologist or project manager; however, I believe that information

assurance professionals will also find this document a ready and adaptable resource.

To get the most from the adapted fill-in-the-blank approach, I recommend attempting to first view each "blank" as though it were an inquiry.

For example, under Integrity Controls I have stated:

> The procedures for updating anti-virus signature files are:
> Procedure X
> Procedure Y
> Procedure Z

Try asking yourself, "What are our procedures for updating anti-virus signature files?" Then, as you pause and answers come flooding to your mind, simply replace 'Procedure X' with the first step of what you or your organization actually does. I have used variations of X, Y, and Z throughout to this template in order to illustrate that more than one response may be necessary.

If answers didn't come flooding to your mind, don't fret. You will find it best to answer each area with existing policy. If you're lucky, your security officer or security program manager has recently updated and published an enterprise information security handbook filled with the best security policies written in lay terms. If you're not so fortunate, you may have to root around in dusty employee handbooks and surf on your static intranet links until you find at least some applicable existing policy. Using existing policy simplifies and hastens coordination issues and ruffles the fewest organizational feathers.

The next best way to answer each blank is with the existing typical organizational or managerial response. If your typical way of handling things is a functional and accepted method, then you have it easy. Just put it in writing. "But wait," you may be thinking, "you want me to document that our friendly termination procedures involve surprise drop offs of empty boxes to the cubes of employees that are to be let go by mid-day?" If that's case, I'd hate to see your unfriendly termination procedures, but you'll have to make that decision. Just remember, others will review this document, so you may wish to quickly revisit your poor public relations campaign and upgrade your procedures to something more palatable before the truth gets out.

Now what if you come across a blank that you've never dealt with? Simple. Invent a response that you feel a reasonable and prudent person would accept, and see where it gets you. The real key to any response is that it is enforceable. The best enforceable responses are those that are documented and known, and thus the cycle of committing all things to paper and spreading the word of the value of current system documentation continues.

Allow your trusted peers to review your initial security plan and ask them for insights. After incorporating their useful responses, you will probably be asked to submit your security plan to your organization's information assurance office. You may find it in your best interest to create a cover letter for all of those who support your efforts to sign off on.

Be committed to your answers, and know that when your document is reviewed, it is not you undergoing a personal confrontation. Rather, the review process is a useful method of weeding out unnecessary information, examining deficiencies, and shaping your system security plan into the tool it is meant to be.

Because organizations may have a preferred format (NIH), I have purposely left this SSP template unnumbered in order to easily accommodate adaptations.

You will likely want to create a cover sheet for your document and include on it the "Name of your Organization," the acknowledgement "Sensitive Information," an "Organizational Logo," the title "System Security Plan for System Name / Identification Number," the current "Date" for versioning purposes, and the statement "Prepared by," to identify who to contact for clarification and to give yourself some credit. Note: The date and the acknowledgement of it containing sensitive information should be on every page.

As you go about gathering information, avoid generic statements, because they do not provide you with thorough documentation. Also, set specific "shall" dates for things not yet accomplished. For example, "The procedures for updating anti-virus signature files shall be listed here by August 31, 2001." Setting specific dates and avoiding the use of generic "all month" dates will let you know where you stand and keep your deliverable schedule on track.

On a parting note, remember, a SSP is a dynamic document reflecting the current security posture of the IT system. Therefore, as further security related information is acquired and as system developments occur, updates to the SPP subject areas should be made.

Works Cited:

Swanson, Marianne. "Special Publication 800-18." NIST Computer Security Resource Center (CSRC). December 1998.
URL: http://csrc.nist.gov/publications/nistpubs/index.html/

OMB. "Management of Federal Information Resources." Circular No. A-130. November 2000.
URL: http://www.whitehouse.gov/omb/circulars/a130/a130appendix_iii.html

GAO. "Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk." GAO / AIMD-98-92. September 1998.
URL: http://www.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=gao&docid=f:ai98092.txt

NIH. "Application / System Security Plan Template." NIH. May 1999.
URL: http://irm.cit.nih.gov/security/secplantemp.html#A

DOJ. "Systems Development Life Cycle Guidance Document." DOJ / IRM / Appendix C-9. March 2000.
URL: http://www.usdoj.gov/jmd/irm/lifecycle/apdxc9.htm

APPENDIX A – USEFUL SYSTEM SECURITY PLAN TEMPLATE

COVER SHEET

The Cover Sheet should contain:

Name of your Organization
Sensitive Information Acknowledgement (on each page)
Organizational Logo
System Security Plan for System Name / Identification Number
Date (on each page)
Prepared by

EXECUTIVE SUMMARY

The Executive Summary should contain:

Introduction
System Purpose
High-level System Overview
Brief References to Applicable Laws / Regulations

TABLE OF CONTENTS

SYSTEM IDENTIFICATION

System Title / System Alias (Acronym)

System X (X)

System Identification Number

Agency/Corporate Acronym-Organization Acronym-GS-System Alias-Number-Year

Responsible Organization

Agency/Corporate Name
Organization Name
Address
Phone

Information Contacts:

System Owner(s)

Person X
Title
Agency/Corporate Name
Organization Name
Address
Phone
Email

System Administrator(s)

Person Y1
Title
Agency/Corporate Name
Organization Name
Address
Phone
Email

Person Y2

Title
Agency/Corporate Name
Organization Name
Address
Phone
Email

System Maintenance

Person Y3
Title
Agency/Corporate Name
Organization Name
Address
Phone
Email

Assignment of Security Responsibility

Person Z
Title
Agency/Corporate Name
Organization Name
Address
Phone
Email

System Operational Status

The following chart depicts the system(s) covered by this SSP and their operational status:

System Name	Under Development	Undergoing a Major Modification	Operational
System X	–	Yes	–

General System Description / Purpose

This system is a General Support System.

The purpose of this system is to…

The process flow of the system is as follows:

1.
2.
3.
4.
5.
6.

The following chart depicts internal and external user organizations and the types of data and processing they utilize:

Organization Name	Internal	External	Types of Data Processing
Organization Y	Yes	–	Data Y

Technical System Environment

The system is located…

The system is connected to…

The system's platform is…

The system's principle components are…

The system uses…

The security software protecting the system is…

System Interconnection / Information Sharing

The following chart depicts interconnected systems, their unique identifiers, whether they have their own SSP, and if an MOU has been obtained:

Interconnected Systems	System Identifiers	SSP	MOU
System Z	ZZZ-YYYY-GS-X-01-2001	Yes	–

Sensitivity of Information Handled

Applicable Laws or Regulations Affecting the System

General Descriptions of Information Sensitivity

The following chart depicts the criticality of the system based on its basic protection requirements:

Protection Requirements	Low	Medium	High
Availability	–	–	Yes
Integrity	–	Yes	–
Confidentiality	–	Yes	–

MANAGEMENT CONTROLS

Risk Assessment and Management

The Risk Assessment methodology used on the system was / will…

The latest Risk Assessment performed on the system was completed on XXXXX YY, 2001.

The next Risk Assessment will performed on the system no later than XXXXX YY, 2004.

Review of Security Controls

The latest independent security review of the system was completed on XXXX YY, 2001.

X performed the security review for the purpose of Y.

The findings of the independent security review show…

As a result of these findings, the following actions have been / will be taken:
Action X
Action Y
Action Z

Rules of Behavior

As the Rules of Behavior will vary greatly between systems let alone organizations, see NIST Special Publication 800-18 for guidance on satisfying this section.

Planning for Security in the Life Cycle

The system is in the X phase of the Life Cycle.

As a system's life cycle will vary greatly between organizations, see NIST Special Publication 800-18 for guidance on satisfying this section.

Accreditation / Authorize Processing

This chart depicts when and who has requested to operate the system and when and who has given their approval for system operation:

Manager Name	Manager Title	Request to Operate	Authorization to Operate
X	X1	XXXXX XX, XXXX	
Y	Y2		XXXXX XX, XXXX

OPERATIONAL CONTROLS

Personnel Controls

The following position(s) have undergone a position sensitivity analysis, and are rated as having High, Moderate, or Low sensitivity:
X Position = High sensitivity
Y Position = Moderate sensitivity

The following position(s) have not yet undergone a position sensitivity analysis:
Z Position = Sensitivity undetermined

The following individuals(s) have undergone background screening appropriate to their position:
Person X
Person Y

The following individuals(s) have not yet undergone background screening appropriate to their position, but shall by the date(s) listed below:
Person Z – April, 13 200? (Date in the near future)

Using the principle of least privilege, user access has been limited to the minimum necessary for the following positions:
X Position
Y Position

The critical function(s) that have been divided among different positions are:
X Position = Ability to X
Y1 Position = Ability to Y1
Y2 Position = Ability to Y2

The critical function(s) that have not yet been divided among different positions, but shall be by the date(s) listed below are:
Z Position = Ability to Z1, Z2, Z3 – Date in the near future

User accounts for this system are requested by…

User accounts for this system are established by…

User accounts for this system are issued by…

User accounts for this system are closed by…

The mechanisms in place for holding users responsible for their actions are:
Mechanism X
Mechanism Y

Mechanism Z

The procedures for friendly terminations are:
Step X
Step Y
Step Z

The procedures for unfriendly terminations are:
Step X
Step Y
Step Z

Physical and Environmental Protection

Entry and exit of personnel from areas containing system hardware, supporting systems, and backup media is restricted by:
Restriction X
Restriction Y

Entry and exit of personnel from areas containing system hardware, supporting systems, and backup media is restricted by:
Restriction Z

The working fire suppression equipment stored near critical systems is accessible by:
Action X, Location X
Action Y, Locations Y, Z
Action Z, Location Z

In case of electrical power failure systems and personnel are protected by:
Option X
Option Y

In case of heating / air-conditioning failure systems and personnel are protected by:
Option X
Option Y

In case of potable water failure personnel are protected by:
Option X
Option Y

In case of sewage failure personnel are protected by:
Option X
Option Y

In case of structural collapse, the systems are protected by:
Option X
Option Y

In case of structural collapse, the systems are protected by:
Option X
Option Y

The only plumbing lines that may endanger the system are located at:
Location X

In case of plumbing leaks, the systems are protected by:
Option X
Option Y

The greatest risk of the potential interception of system data comes from Risk X, and has been addressed by Safeguards X and Y.

Mobile and portable systems are accounted for by:
Method Z

In case of loss or damage, mobile and portable systems and the data they contain are protected by:
Method X
Method Y

Production / Input and Output Controls

The group (help desk) designated to offer advice and support users is Group X, which can be contacted by the following methods:
Method X
Method Y

The procedures for ensuring unauthorized individuals cannot read, copy, alter, or steal printed information are:
Step X
Step Y

The procedures for ensuring unauthorized individuals cannot read, copy, alter, or steal electronic information are:
Step X
Step Y

The procedures for ensuring the restricted access of sensitive system outputs are:
Step X
Step Y

The procedures for ensuring only authorized individuals can pick up, receive, or deliver input and output information and media are:
Step X
Step Y
Step Z

The procedures for controlling the secure transport of system media or output are:
Step X
Step Y

The procedures for controlling the secure mailing of system media or output are:
Step X
Step Y

Sensitivity labeling is accomplished by:
Method X

The following sensitivity / handling label(s) are used frequently:
Label X
Label Y
Label Z

Inventory management is accomplished by:
Method X
Method Y

Media storage protection is accomplished by:
Method X in Location X
Method Y in all other locations

The procedures for sanitizing electronic media for reuse are:
Step X
Step Y

The procedures for destroying unusable electronic media are:
Step X
Step Y

The procedures for shredding or otherwise destroying sensitive hardcopy are:
Step X

Step Y

Continuity of Operations Plan (COOP)

The COOP to allow the continuance of mission-critical functions for this system in case of a catastrophic event involves the following steps:
Step X
Step X1
Step Y
Step Y1
Step Y2
Step Z
Step Z1

The full COOP is accessible via the following personnel / methods:
Person X
Person Y
Person Z
Method X
Method Y

The COOP for this system has been tested by:
Method X
Method Y
Method Z

The COOP for this system was last tested:
Date X

The COOP for this system will next be tested:
Date Y

The COOP(s) to allow the for all supporting IT systems and networks are accessible via the following personnel / methods:
Person X
Person Y
Method X
Method Y

Formal written emergency operating procedures are posted at:
Location X
Location Y

The personnel knowledgeable of and trained in the COOP for this system, and their responsibilities are:

Person X, Responsibility X
Person Y, Responsibility Y
Person Z, Responsibility Y

The written COOP agreements for backup processing are with the following points-of-contact and their respective organizations:
Agreement X, Person X and Contact Information, Organization X
Agreement X, Person Y and Contact Information, Organization X
Agreement Y, Person Z and Contact Information, Organization Y

The procedures and frequency of local backups for this system are:
Step X, Daily, Incremental Backup
Step Y, Monthly, Full Backup

Generational backups are securely stored in the following locations:
Incremental Backups for this fiscal year, On-site Location X
Differential Backups for this fiscal year, On-site Location Y
Full Backups for the last five years, Off-site Location Z

The content of each backup is as follows:
Incremental Backups contain…data types.
Differential Backups contain…data types.
Full Backups contain…data types.

Hardware and System Software Maintenance Controls

The normal restrictions on those who perform maintenance and repair activities are:
Restriction X
Restriction Y

The special procedures to allow for emergency maintenance and repair activities are:
Procedure X
Procedure Y

The procedures used for items serviced through off-site maintenance and repairs are:
Procedure X
Procedure Y

The procedures used for maintenance and repairs via remote maintenance services are:
Procedure X
Procedure Y

The configuration management procedures used for system / software version control are:
Procedure X
Procedure Y

The configuration management procedures used for testing system / software components prior to operation are:
Procedure X
Procedure Y

The configuration management procedures used to ensure continuity of operations plans and other associated data are:
Procedure X
Procedure Y

The configuration management procedures control the usage of test data are:
Procedure X
Procedure Y

The configuration management procedures control the usage of live data are:
Procedure X
Procedure Y

The organizational policies against the illegal use of copyrighted software are…

Integrity Controls

The procedures for updating anti-virus signature files are:
Procedure X
Procedure Y
Procedure Z

The password crackers / checkers used to test password strength are:
Software X
Software Y

The integrity verification programs used to look for data tampering, errors, etc are:
Software X
Software Y

The intrusion detection tools used to identify attacks and do trend analysis are:
Software X
Software Y

The system performance monitoring tools used to analyze system performance are:
Software X
Software Y

The procedures used for system penetration tests are:
Procedure X
Procedure Y

The message authentication and non-repudiation feature of the system is:
Feature X

Documentation

The following chart depicts the types, POCs, and locations of system documentation:

Documentation Type	Vendor	POC	Location
Documentation X	X	Z	Z
COOP	None	Z	Z
–	–	–	–

Security Training, Education, and Awareness

The procedures for ensuring that employees and contractor personnel have been provided system security training are:
Procedure X
Procedure Y

System security training has been provided to the following individuals(s):
Person X
Person Y
Person Z

The procedures for ensuring that employees and contractor personnel are educated in how to recognize and report system security incidents are:
Procedure X
Procedure Y

System security awareness has been promoted by the use of the following methods:
Method X
Method Y
Method Z

The procedures for measuring the effectiveness of system security awareness promotion methods are:
Procedure X
Procedure Y

Incident Response Capability

The procedures for reporting system security incidents are:
Procedure X
Procedure Y
Procedure Z

The person(s) who receive and respond to vendor alerts / advisories are:
Person X
Person Y

The measures planned or in place to prevent system security incidents are:
In Place Measure X
Planned Measure Y
Planned Measure Z

TECHNICAL CONTROLS

Authentication

The authentication methods for the system are:
Method X
Method Y
Method Z

Passwords for the system shall meet the following requirements:
Requirement X
Requirement Y
Requirement Z
Requirement Z1
Requirement Z2

The procedures for verifying that all default authentication mechanism have been disabled or changed are:
Procedure X
Procedure Y

Identification

The identification methods for the system are:
Method X
Method Y
Method Z

Logical Access Controls

The controls in place to authorize the activities of users and system personnel are:
Control X
Control Y
Control Z

The controls in place to restrict the activities of users and system personnel are:
Control X
Control Y
Control Z

The controls in place to detect unauthorized activities of users and system personnel are:
Control X

Control Y
Control Z

Prior to login, the warning banner for this system states:

Audit Trails

System audit trails record the following events:
Auditable Event X
Auditable Event Y
Auditable Event Z

The procedures for ensuring the confidentiality of audit trail data are:
Procedure X
Procedure Y
Procedure Z

System audit trail data is reviewed by Person X every Z.

System audit trail data is reviewed by Person Y every Z1.