DEPARTMENT OF HEALTH & HUMAN SERVICES
Centers for Medicare & Medicaid Services
7500 Security Boulevard, Mail Stop N2-14-26
Baltimore, Maryland 21244-1850

CENTERS FOR MEDICARE & MEDICAID SERVICES (CMS)
Office of Information Services (OIS)
Security and Standards Group (SSG)
7500 Security Blvd
Baltimore, MD 21244-1850

SYSTEM SECURITY PLANS (SSP) METHODOLOGY

Version 3.0
October 28, 2002

Summary of changes in the SSP Methodology v3.0 DRAFT

1. **Global changes to include CMS Business Partner-specific procedures within the methodology.**
2. **Appendix B changed to reflect CMS Information Security Levels Standard, approved on September 27, 2002.**

Summary of changes in the SSP Methodology v2.1

1. **Global change of "GSS and/or MA" to "system" (unless otherwise indicated, this is inclusive of any type of system (Master, GSS, MA or "Other" System)**
2. **Chapter 1.3 Determine System Bountaries reduced from four (4) to three (3) characteristics.**
3. **Chapter 4 sub-sections have been re-organized.**
4. **Table 5 "Authorizing Processing" requirement added.**
5. **Appendix A – Samples deleted (see the CMS IT Security Web Page at http://cms.hhs.gov/it/security)**
6. **SSP Forms and Template Section moved from Chapter 3 to Appendix A**

Appendix A changes:

Certification forms have been consolidated into one (1) form
Accreditation forms have been consolidated into one (1) form
Executive Summary guidance added
1.1 Reference numbers added for FMIB and WST
1.2 Business Owner/Manager added
1.6 Type of System check boxes added
2.5 Additional Comments deleted
3.1.1 IT Related Positions rolled into 3.1
3.1.2 Personnel Screening rolled into 3.1
4.1.1 Passwords rolled into 4.1
4.1.2 Authorization and Access Controls moved to 4.2
4.2.1 Authorization and Access Controls moved from 4.1
4.2.3 Complementary Controls Provided by Support System deleted
4.3.1 Screen Warning Banners rolled into 4.3

Appendix A – primarily applies to GSSs only
Appendix C – Glossary added
Appendix D – Acronyms & Abbreviations added

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This System Security Plans (SSP) Methodology covers all aspects of security for information technology (IT) systems within the scope of the Centers for Medicare & Medicaid Services' (CMS) business functions. It applies to all CMS IT systems and installations, whether developed or maintained in-house or commercially, and to all External Business Partner IT systems and installations operated by or for CMS, e.g., External Business Partner sites. Additionally, the SSP must apply to all employees and personnel from other organizations, including contractor personnel and vendors using or participating in the development, operation and maintenance of CMS IT systems and installations.

This SSP Methodology is to be used by those individuals responsible for IT security at the system level and at the organization level. This document is intended as a guide to be used when creating SSPs. It is written to provide a specific format for an SSP and instructions on the content of the SSP. By following this methodology, one ensures that the SSP developed for one's systems complies with CMS SSP standards. Our goal in writing this document is to lay out the minimum requirements to describe the security protections for our systems and to simplify and minimize the efforts of the developers, maintainers and owners in providing system security plans.

Goal of the System Security Life Cycle

The goal of CMS's system security life cycle is to provide a framework for the protection of its' information and information systems. However, a security plan is not simply a paper exercise by describing implemented protection activities, nor is it developed and then put aside – information risks and vulnerabilities change as rapidly as the technology used to process the information. Security implementation must be a continuous process addressing risks, vulnerabilities, security controls, and performing regular reviews throughout all stages of the system's life cycle. This must be incorporated into the business activities of every entity within the scope of CMS business functions.

Objective of the CMS SSP

The primary objective of the CMS SSP Methodology is to provide IT security guidance to CMS components and its partners in implementing an IT security program that ensures regulatory and standards compliance. It is a tool to be used to ensure continuity of operations and the confidentiality, integrity, availability (CIA), auditability and accountability of information and resources. Specifically, the CMS SSP Methodology is to provide guidance in the preparation of effective security information in order to:

- Protect CMS computer-based information, recognized as a primary government asset, from unauthorized modification, destruction, disruption, or disclosure, whether accidental or intentional.

- Protect information contained in CMS IT systems, and the IT systems and infrastructure themselves.

- Implement the policy requiring the SSP.

- Create a framework for a secure IT environment that meets the requirements of Office of Management and Budget (OMB) A-130, Appendix III; General Accounting Office (GAO), Inspector General (IG), or other external or internal inspection, review or audit; and CMS operational requirements.

This SSP Methodology serves as the standard for all personnel responsible for CMS required SSPs. This methodology supports CMS' policy to provide a comprehensive Information Security (IS) program. This program ensures the existence of adequate safeguards to protect personal, proprietary and other sensitive data in automated systems, and ensures the physical protection of all CMS information and facilities that maintain and/or process CMS data.

The CMS SSP Methodology is based on the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-18, dated December 1998, "Guide for Developing Security Plans for Information Technology Systems". Although the structure of this methodology and the NIST SP 800-18 are very similar, there are some distinct differences between the two documents. Further information on this as well as additional information, resources, and samples for preparing SSPs are available on the CMS IT Security page.

http://cms.hhs.gov/it/security

CHAPTER 1 – CMS SYSTEM SECURITY PLANS METHODOLOGY

1.1 Introduction

CMS uses many assets to accomplish its mission. These include buildings, facilities, communication equipment, computer systems, employees, contractors, public trust, and information. A loss of any one of these assets could affect the quality of support provided by CMS and its' partners to various customers. In particular, CMS needs a system of cost-effective computer security controls to protect its critical IT assets. Additionally, in the fulfillment of its mission, CMS collects information that falls into the category of privacy data, proprietary data, procurement data, inter-agency data, and privileged system information. Established CMS standards in accordance with applicable Federal laws and regulations must protect these types of information. Other directives, regulations, policies, and procedures invoke additional requirements related to the protection of this information. Therefore, CMS has a legal and practical responsibility to maintain the CIA, auditability, and accountability of this information. As a result, CMS has implemented a broad range of standards, policies, procedures, and protective measures to ensure the confidentiality, integrity, and safety of its IT systems, installations, and operations.

CMS information assets have become increasingly more difficult to protect due to advances in technology such as easy-to-use high-level query languages, the use of personal computers, the accelerating use of the Internet and other networks, and general familiarity with data processing. Simply, because new technology is too often adopted before protection measures are developed, these factors have resulted in increased vulnerability of information and information systems. Without a corresponding growth in good data security practices, such advances could result in a higher likelihood of inadvertent or deliberate corruption of CMS information assets and even the loss of the public's trust in CMS's integrity and credibility.

This SSP Methodology is intended to serve as a tool for System Owners/Managers and System Maintainer Managers in determining the SSP requirements of General Support System (GSS), Major Application (MA) and "Other" systems[1]. It is written to provide a specific format for developing an SSP and instructions on the content of the SSP. By following this methodology, one ensures that the SSP developed for one's systems will comply with CMS SSP standards.

The SSP documents the current level of security within the system, including reference to any applicable controls contained in the CMS Master Plan (hereafter referred to as the Master Plan). The SSP documents actual implemented controls not *planned* controls. An IT system is evaluated by the CMS Chief Information Officer (CIO) or his/her Senior Management Official designee (hereafter referred to as the designee) *based on those controls currently implemented and documented in its SSP* to determine whether or not it will be granted authorization to process, i.e. accreditation. Similarly, the SSP forms the primary reference documentation for testing and evaluation, whether by CMS, the GAO, the IG, or other oversight bodies.

Business Partner Note: Business Partner SSPs are not being accredited at this time.

1 The definition for system categories are contained in Section 1.4

1.2 CMS System Security Plans Structure

CMS has implemented a three-tiered hierarchical structure in its SSPs (see Figure 1). At the highest level is the CMS Master Plan. The Master Plan follows the same format as all the SSPs and defines the enterprise-level security controls that are in place within CMS. The Master Plan will contain all the security attributes that are standard enterprise-wide such as personnel controls, physical controls for the site, disaster recovery, etc. What this means is an SSP created for a system inherits the attributes of the Master Plan and needs only to reference it without repeating the details. When the Master Plan is modified all those that are dependent will not have to be changed. This hierarchical structure also applies to any GSS, MA or Other System to which the system is related (see Figure 1). While each system requiring an SSP must develop a separately approved and accredited security plan, the common elements provided in the parent plan are inherited by the subordinate plan by establishing the relationship to a parent system and thus need only reference them if a deviation or exception from the inherited attribute is being made. By doing this, a System Owner/Manager is required only to provide information and protections unique to the particular system for which the SSP is being written.

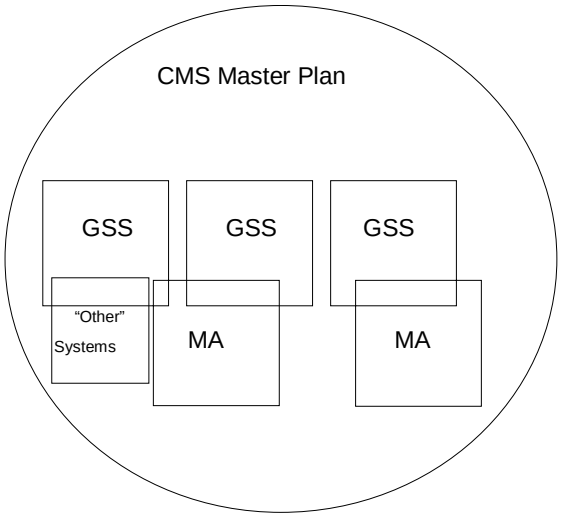


Figure 1 Three-Tier Hierarchical Structure of System Security Plans

The following sections contain guidance to follow in deciding the type of SSP required for a system.

Business Partner Note: CMS has established a 2-Tier Architecture with a General Support System (GSS) as the highest level. The GSS defines any common enterprise level as well as platform level security policies and procedures. External Business Partner system specific details for all controls must be contained in each individual GSS and MA SSP. However, common elements provided in the GSS may be inherited by any subordinate MA or "Other" SSP.

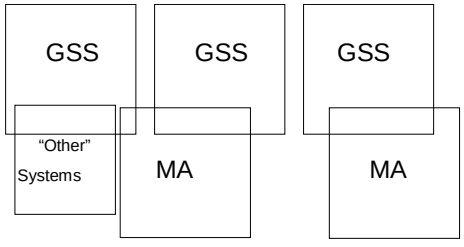


Figure 2 Two-Tier Hierarchical Structure of System Security Plans

1.3 Determine System Boundaries

The first step in implementing the SSP Methodology is defining what constitutes a system and this means determining where its boundaries and interfaces with other systems are. This requires an analysis of both technical system boundaries and organizational responsibilities. Constructing physical and logical boundaries around a set of processes, communications, storage, and related resources, as defined by this document, identifies a system. The set of elements within these boundaries constitutes a single system requiring a security plan. Each component of the system must:

- Be under the same direct management control (i.e., one system owner even though the MA may cross several business lines)
- Have the same general business function(s) or business objective(s)
- Have essentially the same operating characteristics and security needs

All components of a system do not need to be physically connected. Examples:

- a group of stand-alone personal computers (PCs) in an office
- a group of PCs placed in employees homes under defined telecommuting program rules
- a group of portable PCs provided to employees who require mobile computing capability for their jobs
- a system with multiple identical configurations that are installed in locations with the same environmental and physical safeguards

An organization may have systems that differ only in the responsible organization or the physical environment in which they are located. In such instances, it is appropriate and required to use plans that are identical except for those areas of difference. This approach provides coherence and consistent levels of protection for similar systems.

1.4 Determine System Category

The second step in implementing this SSP Methodology is to determine the system's category. Categories include:

- GSS, (e.g., an infrastructure component such the CMS Data Center or WAN Services – Quality Net)
- MA, (e.g., Managed Care Systems, Medicare Beneficiary Enrollment Systems, Fiscal Intermediary Standard System [FISS], Multi Carrier System [MCS])
- Other System (e.g., Adult Immunization)

All Federal systems have some level of sensitivity and require protection as part of good management practice. Therefore, an SSP is required for all CMS systems.

1.4.1 Determine if the System is a GSS

A GSS consists of interconnected information resources under the same direct management control that shares common functionality. A GSS normally includes hardware, software, information, data, applications, communications, facilities, and people and provides general support for a variety of users and/or applications. As a rule of thumb, you can think of a GSS as the physical platform upon which applications run. A GSS, for example, can be a:

- Communications network and ancillary equipment (e.g., WAN Services – Quality Net)
- Departmental data processing center including its' operating system and utilities (e.g., CMS Data Center)

If the system under consideration is a GSS, then it must be determined if it is related to or part of an existing GSS. If so, then the existing GSS SSP must be updated. The System Owner/Manager must adhere to the requirements of the higher level plans (Master Plan/parent GSS plan[s]) or exceptions must be explicitly spelled out. For those areas unique to the individual system, the System Owner/Manager must document the unique information and protections in the system's SSP for those additional or custom areas within the related GSS.

If the GSS does not fall under an existing GSS, then a new GSS SSP will need to be created.

1.4.2 Determine if the System is an MA

Major Applications are systems, usually software applications, that support clearly defined business functions for which there are readily identifiable security considerations and needs (e.g., Managed Care Systems, Medicare Beneficiary Enrollment Systems, FISS, MCS). An MA might be comprised of many individual programs and might have hardware, software, and telecommunications components. These components can be a single software application or a combination of hardware/software focused on supporting a specific business-related function. An MA may also consist of multiple individual applications if all are related to a single business function.

1.4.3 All "Other" Systems

All federal systems have some level of sensitivity and criticality and require protection as part of a good management practice[2].

"Other" systems are those systems that are not classified within an MA. A database application, not covered by an MA SSP, installed and accessed through the Data Center GSS would be considered an "Other" System and require an SSP. Another example would be an application that is part of a pilot and would require an "Other" System SSP.

If these systems are minor, operated and maintained on a local system (e.g., a personal MS Access® database), then an SSP is not required at this time. Also standard commercial off-the-shelf (COTS) software ("shrink-wrap" products such as word processing software, electronic

2 OMB Circular A-130, "Management of Federal Information Resources," Appendix III, "Security of Federal Automated Information Resources"

mail software, utility software, or other general-purpose software) is not considered by itself as a system. COTS products must be documented with the applicable level SSP (e.g., environmental COTS software with GSS, application COTS software with the MA or "Other" System SSP) to which it is associated.

Last, it is important to note that any system that introduces or possesses a feature that compromises or affects the security protections of a system that does have an SSP, or even the CMS environment, must be covered by a security plan. Thus, while an Excel spreadsheet used by five or six budget analysts can be considered a system that does not require an SSP, a personal dial-up modem that can be purchased and installed by a single individual onto his/her workplace desktop certainly does require an approved SSP before it can be made operational. The difference is that the latter can compromise the security of the whole network; the former cannot. A software package that creates persistent browser "cookies" would also impact security, by negating privacy restrictions. Any question about whether a system, however small, requires an SSP should be directed to one's component Information System Security Officer (ISSO).

Business Partner Note: For SSP questions, contact your System Security Officer (SSO).

CHAPTER 2 – POLICY, PRINCIPLES and REFERENCES

2.1 General Policies

It is the policy of CMS to safeguard information contained in IT systems and installations through the implementation of an agency-wide computer security program. Table 1 below lists the objectives associated with the implementation of CMS's IS Program.

Table 1. OBJECTIVES

1) Establish a level of security for all information technology systems and installations commensurate with the sensitivity of the information, with the associated risk, and the magnitude of loss or harm that could result from the loss, misuse, disclosure, or modification of the information contained in the information technology systems or installations. Each system's level of security must protect the confidentiality, integrity, and availability of the information. Specifically, this requires that: ▪ Each CMS information technology system and installation has the appropriate technical, personnel, administrative, environmental, and telecommunications safeguards. ▪ IT security be cost effective. ▪ Each CMS information technology application and installation categorized as a GSS, MA or Other System is covered by an accredited SSP. ▪ Each CMS component implements and administers an IT security program that meets statutory, regulatory, and Departmental requirements; the needs of CMS; and the public. ▪ Assure that only authorized personnel have access to CMS information technology systems, data and installations.
2) Develop and test plans to provide CMS information technology systems and installations with reasonable continuity of support should their normal operations be disrupted.
3) Use national and federal information processing and telecommunications standards, such as the Federal Information Processing Standards (FIPS) or as promulgated by the NIST, except where it can be demonstrated that the costs of using a standard exceeds the benefits or that the standard will impede CMS in accomplishing its' mission.
4) Develop and maintain an organization-wide database of information technology systems and installations that includes the current security status and the sensitivity levels of information being processed.
5) Establish IT security awareness and training for managers and staff, who have management, administrative, operational, maintenance, support, or user responsibilities, related to CMS information technology systems or installations.
6) Ensure proper use of CMS's information technology systems and installations, which have been established for conducting official CMS business.
7) Anyone with access to CMS Computer Systems containing sensitive information must abide by the following: [3] ▪ Do not disclose or lend you IDENTIFICATION NUMBER AND/ OR PASSWORD to someone else. They are for your use only and serve as your "electronic signature." This means that you may be held responsible for the consequences of unauthorized or illegal transactions. ▪ Do not browse or use CMS data files for unauthorized or illegal purposes. ▪ Do not use CMS data files for private gain or to misrepresent yourself or CMS. ▪ Do not make any disclosure of CMS data that is not specifically authorized. ▪ Do not duplicate CMS data files, create sub-files of such records, remove or transmit data unless you have been specifically authorized to do so.

[3] Master Labor Agreement (Between CMS and AFGE dated March 8, 1998), Article 35 - Computer Security

Table 1. OBJECTIVES

▪ Do not change, delete, or otherwise alter CMS data files unless you have been specifically authorized to do so. ▪ Do not make copies of data files, with identifiable data, or data that would allow individual identities to be deduced unless you have been specifically authorized to do so. ▪ Do not intentionally cause corruption or disruption of CMS data files. A violation of these security requirements could result in termination of systems access privileges and/or disciplinary/adverse action up to and including removal from Federal Service, depending upon the seriousness of the offense. In addition, Federal, State, and/or local laws may provide criminal penalties for any person illegally accessing or using a Government-owned or operated computer system illegally.
8) CMS encourages its employees to use the Internet to accomplish job responsibilities and further business goals. Excessive use, e.g., "surfing the Internet", for non-work related goals, during working hours is prohibited.

2.2 General and User Principles

In accordance with the general organization-wide security policies, CMS abides by the general and user principles listed in Table 2 below.

Table 2. GENERAL and USER PRINCIPLES

General Principles
1) The IT security program is an integral element of sound management and directly supports the mission of CMS by protecting its critical physical and financial resources, reputation, legal position, and employees.
2) Effective IT security requires a comprehensive and integrated approach that considers a variety of areas, both within and outside of the IT security field, including such factors as system management, legal issues, quality assurance, as well as internal and management controls.
3) Government-owned or leased IT resources are accessible for audit at anytime; when using such government equipment, an employee or user must be aware in those audit situations, authorized individuals will have access to their information.
4) IT security must be cost effective; the level of security must be appropriate and proportionate to the value of the IT systems, the degree of reliance on the IT systems, and the probability and extent of potential harm.
5) The responsibility and accountability of System Owners/Managers, providers, users of CMS information technology systems and other parties must be explicitly and formally expressed.
6) CMS System Owner/Managers have security responsibilities outside their own organizations. If a CMS system has external connections, including users, its System Owner/Managers have a responsibility to share appropriate knowledge about the existence and general extent of security measures, so that other users can be confident that the system is adequately secure.
7) IT security must be periodically reassessed because computers, technology, threats, vulnerabilities, and the environments in which they operate are dynamic.

Table 2. GENERAL and USER PRINCIPLES

General Principles
8) Computer security is constrained by societal factors, such as employee's concerns about privacy and confidentiality of their personal data in the work place. Security controls will be selected and implemented with recognition of the rights and legitimate interests of others. This involves balancing the security needs of information owners and users with societal goals.
9) All CMS information technology systems, installations, and applications will comply with the IT security requirements contained in the following: OMB Circular No. A-130, Appendix III, Security of Federal Automated Information Resources and NIST 800-18, "Guide for Developing Security Plans for Information Technology Systems".
User Principles
1) Each user will have a unique user Identification (ID) issued to them for accountability reasons and will be assigned only the least privileged access rights or privileges needed to perform their tasks. User IDs will not be shared. Additionally, the unique user ID must be safeguarded to preclude unauthorized use of information systems, as well as protecting the user.
2) Users are responsible and will be held individually accountable for all actions performed under their user ID.
3) Each user will have a unique password issued to them to authenticate a specific user ID and ensure access to information system resources is protected. The unique password, in conjunction with the unique user ID, allows authorized personnel system access, precluding unauthorized tampering with CMS information assets. Passwords must not be shared, even with other authorized users.
4) Users must protect their equipment by keeping their equipment in a secure environment. Users must keep food, drink, and other hazards far away from their equipment.
5) Users must protect their area by keeping unauthorized individuals away from their equipment and data.
6) Users must protect their data and files by always preventing unauthorized access to their data and files.
7) Users must protect their storage media by not leaving their storage media lying around and locking up their storage media.
8) Users must protect data by backing up frequently and always keeping back-ups in a secure location.
9) Users must protect against computer viruses by never using unauthorized software. They must receive management approval from the Office responsible for the operating platform prior to loading any new software onto any CMS IT systems. They must scan all new software or diskettes received from any source prior to introducing them to any CMS IT system.

2.3 References

This SSP Methodology used many references in its development. These references, in their entirety, may be useful in the development of a CMS SSP and are listed in Table 3 below.

Table 3. LIST OF REFERENCES

REFERENCES

Table 3. LIST OF REFERENCES

REFERENCES
Public Law 93-579, The Privacy Act of 1974, as amended.
Public Law 99-474, *Computer Fraud & Abuse Act of 1986.*
Public Law 100-235, *Computer Security Act of 1987.*
Public Law 104-106, *Clinger-Cohen Act of 1996* (formerly called *Information Technology Management Reform Act*).
Freedom of Information Act (FOIA) of 1974, as amended by Public Law 104-231, *Electronic Freedom of Information Act of 1996.*
Public Law 106-398, *National Defense Authorization Fiscal Year 2001, Government Information Security Reform Act (GISRA) of 2000.*
Public Law 104-13, *Paperwork Reduction Act of 1978*, as amended in 1995, U.S. Code 44 Chapter 35.
Public Law 104-191, *Health Insurance Portability and Accountability Act (HIPAA)*, 1996.
Public Law 74-271, *Social Security Act*, as amended, §1816, Use of public agencies or private organizations to facilitate payment to providers of services.
Public Law 74-271, *Social Security Act*, as amended, §1842, Use of carriers for administration of benefits.
Presidential Decision Directive/NSC-63 (PDD 63), *Critical Infrastructure Protection*, May 22, 1998.
Office of Management and Budget (OMB) Circular No. A-123, *Management Accountability and Control*, June 21, 1995.
OMB Circular No. A-127, *Financial Management Systems*, Transmittal 2, June 10, 1999.
OMB Circular A-130, *Management of Federal Information Resources*, Transmittal 4, November 28, 2000.
Appendix III to OMB Circular No. A-130, *Security of Federal Automated Information Resources*, November 28, 2000.
GAO/AIMD-12.19.6, *Federal Information System Controls Audit Manual (FISCAM)*, January 1999.
IRS Publication 1075, *Tax Information Security Guidelines for Federal, State, and Local Agencies*, June 2000.
NIST Special Publication 800-18, Guide for Developing Security Plans for IT Systems, December 1998.

CHAPTER 3 – SYSTEM SECURITY PLANS FORMS and INSTRUCTIONS

3.1 SSP Documentation

To create a usable and functional SSP, the System Owner/Manager must keep the SSP package in a three ring binder. Placing all IS documentation in a loose-leaf binder provides several benefits. First, it is important that a history of all documentation and sign-offs related to the security planning process be maintained. Secondly, using a binder for the package facilitates the update and review processes by allowing the distribution of portions of the SSP rather than the entire SSP. Since the SSP is Sensitive but Unclassified (SBU), the binder makes it much easier to segregate sensitive portions that must not be made widely available (e.g., confidentiality issues contained within Contingency Plans). This format also promotes change management by facilitating the separation of those sections that change frequently in appendices (e.g., equipment lists) that can be updated through issuing updated addendum or replacing outdated appendices with new ones.

3.2 System Security Plan Sections

The SSP documents controls that are tested and implemented to provide protection from threats and vulnerabilities identified during the planning and review process. At a minimum, it must include the following sections with associated information:

- **Section 1, System Identification** – official name and/or title of system, including acronym, responsible organization, information contacts, assignment of responsibility, and system operational status and general description and purpose.
- **Section 2, Management Controls** – overall management controls currently implemented including risk assessment/management, review of security controls, rules of behavior, review of audit logs, testing mandates, and planning for security in the system development lifecycle.
- **Section 3, Operational Controls** – day-to-day procedures and mechanisms such as personnel security, physical and environmental protection, hardware and application software maintenance controls, data integrity/validation controls, documentation, and system security awareness training.
- **Section 4, Technical Controls** – user identification and authentication, authorization and access controls, remote users and dial-up, wide area networks (WAN) controls, public access controls, test scripts and results and audit trails.
- **Section 5, Appendices & Attachments** – relevant supporting documentation.

3.3 SSP Template

The document outline for an SSP is provided in Appendix A. This template serves as a generic model SSP for any system and provides the minimum requirements for an SSP. This model in conjunction with implementation guidance (Chapter 4 of this document) and other reference materials contained in Appendix B, C and D assists a System Owner/Manager in developing an SSP as well as facilitating the proper maintenance of the SSP during the system's life cycle. Higher-level SSP controls should not be repeated except when enhanced or modified. This will reduce the volume of each SSP and the maintenance overhead for all SSPs.

3.4 Packaging of the SSP

The SSP package consists of four major tabs.

TAB A. CMS SSP CERTIFICATION FORM. Tab (A) contains the system certification form signed by the component ISSO/SSO, System Owner/Manager, and System Maintainer Manager. The certification form and signatures attest to the fact that the system has been examined for the adequacy of controls implemented and considers them satisfactory in meeting agency policy and the component's business requirements. Note: Certification and accreditation depends on the controls implemented and tested as of the date of sign-off. No changes to the security posture can be made without retesting, recertification and reaccreditation. For an explanation of how this form is to be used in the SSP process, see section 4.6, Certification Reviews.

TAB B. CMS SSP ACCREDITATION FORM. Tab (B) contains the system accreditation form signed by the CMS CIO or designee. This accreditation form and signature provides the proper documentation verifying that the system has been examined by the authorizing official for the adequacy of controls implemented and considers them satisfactory in meeting agency policy to grant either interim or full authorization to process. Interim Approval to Process is used when CMS's CIO grants approval to process but with certain limitations due to the level of risk currently in the system. Authorization to Process is required for new systems, after major system modifications, when the data sensitivity level increases, after a serious security violation, due to changes in the threat environment, or when the previous accreditation expires. For an explanation of how this form is to be used in the SSP process, see section 4.7, System Accreditation.

Business Partner Note: Business Partner SSPs are not being accredited at this time.

TAB C. SYSTEM SECURITY PLAN, APPLICABLE APPENDICES and ATTACHMENTS. Tab (C) is the actual SSP and associated appendices (e.g., equipment lists) and attachments (e.g., risk assessment.) The contents of this tab must follow the SSP outline provided in Appendix A of this methodology.

TAB D. SUMMARIES, REVIEWS AND REFERENCES. Tab (D) contains summaries and references to the documentation produced during the periodic security control reviews. For initial SSPs, this tab may not contain any documents. As systems' security documentation is maintained, this tab will include prior SSPs and the summary documentation developed for each security review.

NOTE: The cover page of the SSP and the footer of all the subsequent pages (excluding the appendices and attachments) must include the date of the SSP and the SSP version number. The cover should also include the version number and date of the CMS SSP Methodology used to develop the SSP. Pages must be numbered, with each page showing the current page number and total number of pages, e.g., Page 3 of 16." This type of page numbering assists the reader in determining if the SSP they are reviewing is complete.

CHAPTER 4 – GENERAL IMPLEMENTATION GUIDANCE

This section of the SSP Methodology is intended to provide general guidance on:

- System Owner/Manager's responsibilities
- Developing an SSP
- Reviewing and updating an SSP
- Determining mandatory security controls for all systems
- Certifying a system
- Authorizing the use of a system (Accreditation)
- Performing risk management activities

4.1 Mandatory Security Controls for All Systems

All CMS employees and contractors are responsible for ensuring that CMS's information is adequately protected. OMB Circular A-130, Appendix III prescribes the security controls that must be implemented to protect information resources. These security controls apply to all systems. These controls are as follows:

Table 5. MANDATORY SECURITY CONTROLS

Type of Control	Description
Assigning Responsibility	Responsibility for security in each system must be assigned in writing. The individual(s) responsible for a GSS must be knowledgeable of the technology used by the system and in providing security for that type of technology. The individual(s) responsible for an MA or "Other" system must have an understanding of the types of information and processes supported by the application and the controls used in securing the application.
Planning for Security	Security planning requirements apply to all stages of the system/application life cycle from pre-development and development through post development activities. Planning for security, at the onset of the system and application life cycle, is especially important. This plan ensures that all security requirements are identified and that vulnerabilities are not introduced as the system is developed, implemented, and maintained.
Reviewing Security Controls	A review of security controls at least every year is required to be performed for all systems. The scope and frequency of the review or audit must be commensurate with the acceptable level of risk to the system.
Authorizing Processing	All systems must be authorized in writing to process by the CIO or designee based on the implementation of its SSP before beginning or significantly changing processing in the system. Use of the system shall be authorized every year for all systems.

4.2 Federal Manager's Financial Integrity Act (FMFIA) & OMB Circular A-123

Depending on the risk and magnitude of harm that could result, a deficiency or material weakness must be identified and documented pursuant to OMB Circular A-123 and the FMFIA for both GSSs and MAs, if the following components are not in place: formal (i.e., written) assignment of responsibility; a workable SSP; or written management approval to operate.

In addition, documentation must provide information about the last audits or reviews of the system within the last 12 months, including who performed the review, when the review was performed, the purpose of the review, the general findings, and any actions taken as a result of the review. An indication must be made if an independent audit or review has not been conducted on this system.

4.3 System Owner/Manager's Responsibilities

The System Owner/Manager must be a CMS group director or above. System Owner/Managers are responsible for completing all CMS and Federal requirements for identifying their system and preparing SSPs that provide a description of the security and privacy requirements of the subject system and the System Owner/Manager's plan for meeting those requirements. System Owners/Managers are responsible for conducting risk assessments, implementing controls determined to be required and cost-effective, and developing contingency and disaster recovery plans that ensure availability of the system for mission accomplishment.

System Owners/Managers must complete all requirements for certification. Once an SSP is created for a system, the System Owner/Manager's, System Maintainer Manager's and the Component ISSO's/SSO's signatures on the certification form, attest to the fact that they have examined the controls implemented and tested and consider them adequate to meet agency IT security needs. As indicated, the System Maintainer Manager and Component's ISSO/SSO are signing the certification form but it is the sole responsibility of the System Owner/Manager to ensure that the proper controls have been identified, documented in the SSP and implemented for the system.

It is also the responsibility of the System Owner/Manager to submit the completed SSP binder to the Office of Information Services (OIS), Security and Standards Group (SSG) for CMS CIO accreditation. The SSP binder must contain:

- TAB A – a completed Certification form signed by all relevant parties
- TAB B – a completed Accreditation form with the name of the system and the name of the CMS component and System Owner/Manager responsible for the system
- TAB C – the completed SSP and including all relevant appendices and attachments
- TAB D – any relevant documentation produced during periodic security reviews, if applicable

The complete SSP package (Tabs A-D) for the system is used as the foundation for the accreditation.

Business Partner Note:
1. The System Owner/Manager must be the Vice President of Medicare Operations or equivalent.
2. Business Partner SSPs are not being accredited at this time.

3. Business Partners need only send the original signed certification form.

4.4 SSP Development

An SSP does not necessarily have to be developed from scratch; much of the needed material may already be available in other system documentation. System manuals, contingency plans, and security-related documentation are examples of documentation that may contain some of the material needed for the SSP. In addition, keep in mind that if the documentation already exists, and is up-to-date, it can be summarized and referenced in the SSP. Our goal is for SSPs to be as short as possible yet contain the critical security-relevant information.

Once completed, an SSP must contain technical information about the system, its security requirements and the controls implemented to provide protection against its vulnerabilities. All SSPs must be dated to allow ease of tracking modifications and approvals (every page must have date, version number, page number, and total number of pages on it.)

4.5 Reviewing and Updating an SSP

The security of a system may degrade over time as the technology changes, the system evolves, changes occur to authorizing legislation or requirements, or people and procedures change. Periodic reviews provide assurance that management, operations, personnel, and technical controls are functioning effectively, providing adequate levels of protection.

OMB requires, at least every year, that a review or security audit be conducted for all systems. These reviews or audits are in addition to system testing and the types of reviews conducted as part of the risk management program. The objective of these reviews is to provide verification that the controls selected and/or installed are adequate to provide a level of protection to reach an acceptable level of risk to operate for the system. The determination of the level of risk acceptable must be relative to the system requirements for CIA, as well as the identified threats. The scope of the review or audit should be commensurate with the level of risk and/or threat to the system.

4.6 Certification Reviews

Certification review is a requirement for all CMS systems. Certification is based on a technical evaluation of a system to see how well it meets its' security requirements. Initial certification must be completed within the component before the system can be forwarded for accreditation review. The component ISSO/SSO, System Owner/Manager, and System Maintainer Manager must examine the controls implemented for the system and attest to the successful completion of the appropriate technical certification evaluations.

Systems must be re-certified when:

- substantial changes are made to the system
- changes in requirements result in the need to process data of a higher sensitivity
- changes occur to authorizing legislation or Federal requirements
- after the occurrence of a serious security violation which raises questions about the validity of an earlier certification
- expiration of previous certification or accreditation

The Certification Form will be completed and signed by the component ISSO/SSO, System Owner/Manager, and the System Maintainer Manager. The Certification Restrictions page must state any restrictions on use of the system that are being self-imposed by the system owner. The Certification Actions page is also completed by the System Owner/Manager and will list all the *planned* enhancements to the system and the anticipated completion dates.

4.7 System Accreditation

The CMS CIO or the designee must authorize in writing the use of each system. This official cannot be the person assigned responsibility for the security of the system. Accreditation must be based on the SSP documentation and certification forms.

All CMS systems must receive formal management approval to process by the CMS CIO or designee. The SSP and supporting documentation will be evaluated based on an acceptable level of risk and a decision to accredit or not accredit will be made. A system being accredited indicates that a satisfactory level of operational security is present. The CMS CIO or designee signs a formal accreditation statement declaring that the system appears to be operating at an acceptable level of risk to grant approval to process. A system not being accredited indicates that the level of risk either has not been adequately defined or reduced to an acceptable level for operational requirements.

Conditional management approval to process can be granted for a fixed period of time, not to exceed one year. This authority is based on an approved SSP and is contingent on certain conditions being met. The interim approval to operate, while continuing the management authorization process, permits the system to meet its operational business requirements while improving its computer security posture. If the CMS CIO or the designee is not satisfied that the system is protected at an acceptable level of risk, an interim accreditation can be granted to allow time for implementation of additional controls. Interim approval can only be granted by the CMS CIO or the designee in lieu of a full denial to process. Interim approval to operate is not a waiver of the requirement for management approval to process. The system must meet all requirements and receive management approval to process by the interim approval expiration date. No extensions of interim accreditation can be granted except by the CMS CIO or the designee.

An accreditation to process must be requested after any of the conditions as listed in section 4.6 above.

Business Partner note: CMS CIO accreditation does not apply to Business Partners at this time.

4.8 Risk Management Activities

Risk assessment and risk management are crucial elements of the IS process. These activities include identification of: informational and other assets of the system; threats that could affect the CIA, auditability and accountability of the system; important system vulnerabilities to the threats; potential impacts from threat activity; protection requirements to control the risks; and selection of appropriate security measures. The following risk management activities must be completed and be included in the SSP for a system:

- Identify the sensitivity of the information processed
- Assess the risks and magnitude of harm that would result from the loss, misuse, or unauthorized access to, or modification of the information in the application or system
- Determine what constitutes adequate security

The security of each application that processes on a GSS may affect the security of other applications sharing the GSS. One of the roles of GSS security is to ensure separation of applications such that the potential for one application to adversely affect another is minimized. The GSS has no responsibility to provide security beyond their own system protection levels, unless specifically requested by the application managers.

Simply implementing additional security controls does not ensure security. Security controls and products must be tested to ensure they work and are being used correctly or the security control may represent an additional area of vulnerability for the system. New or additional security controls must follow the standard application development process: specification, design, and testing.

The results of the risk assessment, using the CMS IS Risk Assessment Methodology, must be documented and provided in the SSP. Further information can be found at the CMS IS web site, http://cms.hhs.gov/it/security. The CIO or designee will take this information into consideration when reviewing the system for accreditation. Assessing the risk to a system will be an on-going activity to ensure that new threats and vulnerabilities are identified and appropriate security measures are implemented.

CHAPTER 5 – SYSTEM SECURITY PLAN LIFE CYCLE

5.1 Introduction to System Development Life Cycle (SDLC)

The implementation of an effective IS process begins at the start of the SDLC process and culminates with the retirement of a system. During the SDLC, security information is developed throughout the lifecycle, resulting in the actual SSP deliverable prior to implementation of the production system. To understand the application of this SSP Methodology to the system life cycle, one must first understand the CMS SDLC phases. A brief overview of the CMS SDLC is provided in the paragraphs below.

Business Partner note: Business Partners should review the following CMS SDLC phases, along with the SDLC actions in Figure 3, to assist them in describing in their SSP how their Corporate life cycle process/methodology implements IS.

5.2 CMS SDLC Overview

The CMS SDLC is presented as three life cycle phases and a series of activities that transpire within each phase. The grouping of activities into three life cycle phases is simply based on those activities that take place prior to development, those that take place during development, and those that take place after development. The three phases are naturally named:

- Pre-Development Phase
- Development Phase

- Post-Development Phase

The description of the activities that are required in each life cycle phase is presented in this grouping. These life cycle phases and activities represent the series of activities that occur throughout a system's lifetime, from beginning to end. All of these activities occur in sequence within each life cycle phase, but within the Development Phase, the sequence will usually be iterated several times depending upon the development strategy.

For the purpose of this document, the SSP requirements, controls, and deliverables associated with each of the CMS SDLC must be addressed. For further explanation of CMS's SDLC, refer to the CMS SDLC.

5.3 System Security Plan Life Cycle

The SSP life cycle closely follows the SDLC. Each of the life cycle phases is discussed below.

5.3.1 Pre-Development Phase

During the pre-development phase, the need for a system is expressed and the purpose of the system is documented. An information sensitivity assessment must be performed to look at the sensitivity of the information to be processed and the system itself. The sensitivity and criticality of the information stored within, processed by, or transmitted by the system provides the basis for the value of the system and is one of the major factors in risk management. An initial risk assessment must be prepared during this phase. System planners define the requirements for the system and security requirements must also be developed at the same time. These requirements can be expressed as technical features (e.g., access controls), assurances (e.g., developers granted only on-site access to the CMSnet), or operational practices (e.g., awareness and training). Initiation of the security plan is based on available information at the onset of the SDLC process.

5.3.2 Development Phase

During the development phase, the system is designed, purchased, programmed, developed, or otherwise constructed. During this phase, the security plan must be functional as the phase approaches its end. Changes must continue to be made as the system matures and technology changes. Security questions that must be addressed include:

- During the system design, were security requirements identified?
- Were the appropriate security controls, with associated evaluation and test procedures, developed before the procurement action?
- Did the solicitation documents include security requirements and evaluations/test procedures?
- Did the requirements permit updating security requirements as new threats/vulnerabilities are identified and as new technologies are implemented?
- Have additional risks identified during the development phase been reflected in the existing

risk assessment and have plans addressed risk management? Have other risks been mitigated by the development and if so, has the risk assessment been updated to reflect the change in risk management?

The system's security features must be configured and enabled, the system must be tested and installed or fielded, and the system must be authorized for processing. A design review and systems test must be performed prior to placing the system into operation, to ensure that it meets security specifications. These activities support or coincide with the certification and accreditation activities all systems must undergo to ensure security compliance. System certification is typically performed by the System Owner/Manager/Maintainer, or designee, as a management control. Accrediting a system must be performed or overseen by the CMS CIO or designee. Additionally, if new controls are added to the application or support system, additional acceptance tests of those new controls must be performed. This ensures that new controls meet security specifications and do not conflict with or invalidate existing controls. At the end of this phase the security plan must be complete and functional.

5.3.3 Post Development Phase

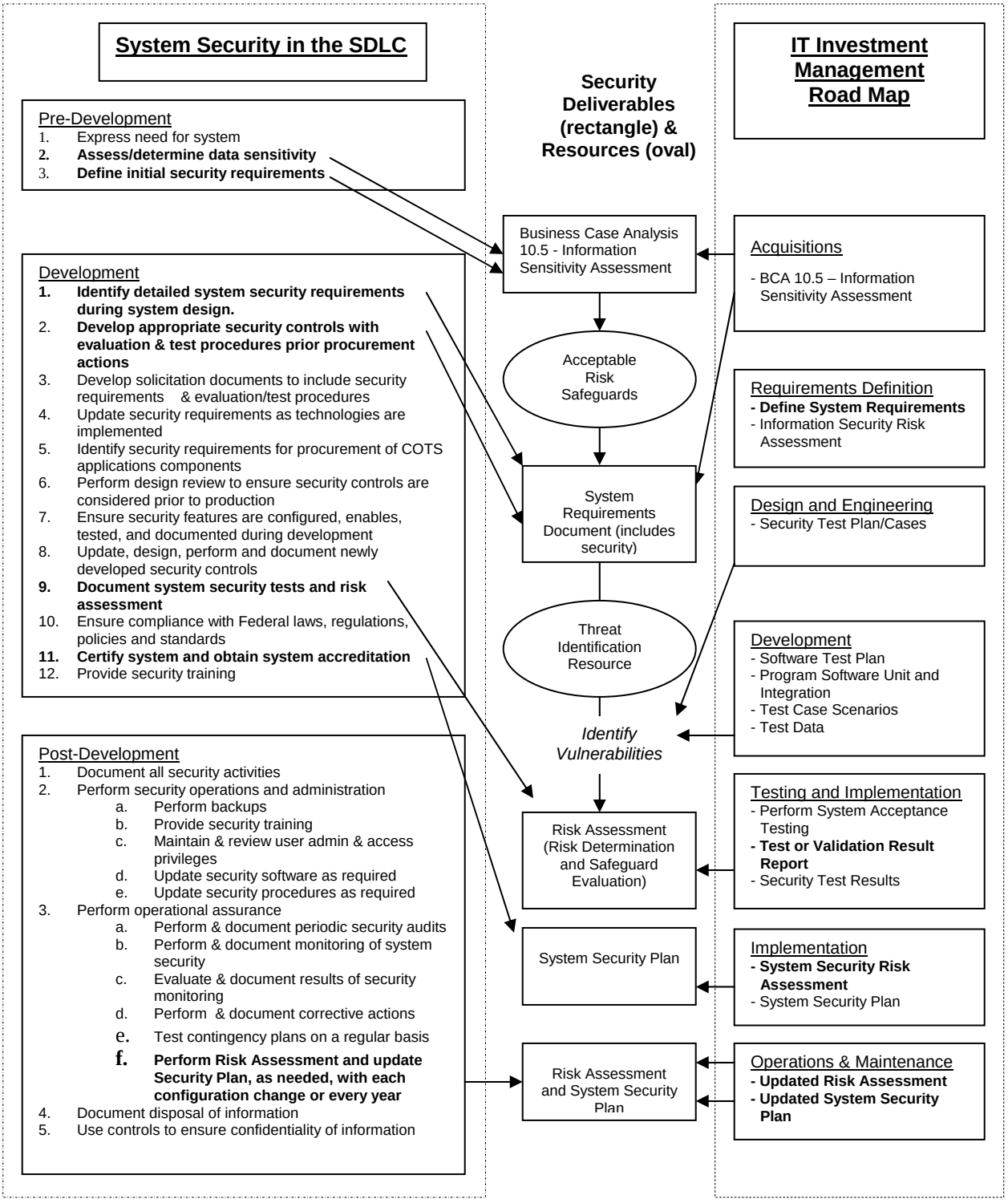
During this phase, the system performs its work. If the system undergoes modifications, any changes to security activities must be documented in the security plan. These changes include level of risk, management of the risk, and mitigation and/or elimination of existing risks. In the security plan, security operations and administration, operational assurance, and audits and monitoring must be described. During this phase of the SDLC the security plan must be the most complete and only change with modifications in systems or policy.

This phase of the life cycle involves the disposition of information, hardware, and software when the system is at the completion of its utilization. Before final destruction of the SSP, verification of any federal records retention period requirement must be investigated. At the completion of a systems life cycle (disposal of a system), the security plan, including every accredited version, must be archived in accordance with Federal records archiving requirements.

5.4 Crosswalk of SDLC with SSP Life Cycle Actions

Figure 3 graphically represents each of the SDLC phases with the specific security actions that need to occur during that phase of the SDLC.

Figure 3. Security in the System Development Life Cycle and CMS' Roadmap



APPENDIX A – CMS SSP Template

NOTE: This template lists all the security relevant issues and protections pertaining to the system. A particular system may inherit many, and in some cases, all, of the issues and protections from an SSP above it in the hierarchy. In such a case, only exceptions, modifications, or deviations from the inherited properties need be noted in the SSP. An SSP for a system that poses no new security risks and has no new security protections may thus be as short as a few pages, with most of those being signature pages. Our goal is to reduce to the minimum the effort needed by developers to produce functioning, workable systems.

TAB A: CMS SSP Certification Form

✓	**Certification is required for the following reason(s):**
	New System
	Major system modification
	Increased system data sensitivity level
	Serious security violation
	Changes in the threat environment
	Expired Certification/Accreditation

The signatures below attest that the appropriate technical certification evaluations have been conducted successfully.

_____

Name of System

_____

CMS Component/Business Partner Name

(printed name)_____(signature)_____
CMS Component Information System Security Officer (ISSO)/
System Security Officer (SSO) **Date**

I, the System Owner/Manager/Maintainer, have examined the controls implemented for this system and consider them adequate to meet agency policy and the relevant business requirements. I also understand and accept the risk inherent in processing on a network or at the installation(s) that supports this system, particularly where the support system is operated outside of my management control. This certification is based on the documented results of the design reviews, system test and the recommendations of the testing teams.

(printed name)_____(signature)_____
System Owner/Manager **Date**

(printed name)_____(signature)_____
System Maintainer Manager **Date**

Certification Restrictions

Certification is granted with the following restrictions (use additional pages if necessary):

NOTE: If no certifications restrictions apply add the following "No Restrictions Apply".

Certification Actions

The following specific actions are to be completed by the dates indicated (use additional pages if necessary):

NOTE: If no certifications Actions apply add the following "No Actions Apply".

TAB B: CMS SSP Accreditation Form

___ Accreditation

___ Interim Accreditation

✓	**Accreditation is required for the following reason(s):**
	New System
	Major system modification
	Increased system data sensitivity level
	Serious security violation
	Changes in the threat environment
	Expired Accreditation

A The signature below attests to the (___ approval ___ denial) of formal management approval to process (system accreditation) based on the conditions listed in attachments B and C for the system listed below. This approval to process expires at close of business on _____.

_____

Name of System

_____

CMS Component **System Owner/Manager (name)**

I, the CMS CIO (or his/her Senior Management Official Designee) have examined the controls implemented for this system and consider them (___ adequate ___ not adequate) to meet agency policy and the system appears to be operating at an (___ acceptable ___ unacceptable) level or risk.

(printed name)_____(signature)_____
CMS CIO or Senior Management Official Designee **Date**

Accreditation Restrictions

Accreditation is granted with the following restrictions (use additional pages if necessary):

C

Accreditation Actions

The following specific actions are to be completed by the dates indicated (use additional pages if necessary):

TAB C: CMS SSP TEMPLATE

Executive Summary

An Executive Summary is **OPTIONAL**. If included, provide a summary of each of the first four (4) sections of the SSP. Do not restate methodology, only provide a summary of facts about the system being documented. If an executive summary is included with the SSP, it must be no more than one (1) single spaced page in length.

DATE: (of plan or modification)
METHODOLOGY DATE/VERSION: (used to write the SSP)

Section 1. SYSTEM IDENTIFICATION

1.1 System Name/Title

Official System Name: (Use official CMS system/name or identifier) System Acronym: (Use official CMS acronym) *Note: Please include any of these numbers if applicable. State N/A for non-applicable items.* System of Records (SOR) #: Financial Management Investment Board (FMIB) #: Web Support Team (WST) #:

1.2 Responsible Organization

In this section, list the CMS organizational component responsible for the system. If another contractor performs the function, identify the Business Partner and/or other organization, and describe the relationship. Be specific about the organization and do not abbreviate. Include all physical locations and addresses.

Name of Organization: Address: City, State Zip: Contract Number, Contractor Name (if applicable):

1.3 Information Contact(s)

CMS requires that all four (4) of the following information contacts be included and completed as shown below. The System Owner/Manager must be the VP for Medicare Operations and the Business Owner/Manager should be indicated as "N/A".

Name (System Owner/Manager): Title: Organization: Address: Mailstop: City, State Zip: Email address: Phone number:	Name (Business Owner/Manager[s]) [4]: Title: Organization: Address: Mailstop: City, State Zip: Email address: Phone number:

4 There may be several Business Owner/Manager(s) (other than the System Owner/Manager), but the System Owner/Manager is the sole owner of the system

Name (SSP Author): Title: Organization: Address: Mailstop: City, State Zip: Email address: Phone number:	Name (System Maintainer Manager): Title: Organization: Address: Mailstop: City, State Zip: Email Address: Phone number:

1.4 Assignment of Security Responsibility

This section requires four (4) different security contacts—two (2) different security contacts and two (2) different emergency contacts. Each emergency contact should know how to contact the primary contact or his/her supervisor but does not have to be a technical person.

Name (individual[s] responsible for security):
Title:
Organization:
Address:
Mailstop:
City, State Zip:
Email Address:
Telephone number:
Emergency Contact Information (name, phone and email only):

Name (Component Information System Security Officer/System Security Officer):
Title:
Organization:
Address:
Mailstop:
City, State Zip:
Email Address:
Phone number:
Emergency contact information (name, phone and email only):

Include or attach a copy of written appointment of responsibility to the individual(s)

1.5 System Operational Status ✓

Document the operational status of the system: _____ new, _____ operational, or _____ undergoing a major modification.

1.6 General Description/Purpose

Check Type of System(s) ✓		
CMS On-site	***CMS Off-site***	***Business Partners (Medicare Contractors)***
_____ *Master (OIS-SSG use only)*		
_____ *GSS*	_____ *GSS*	_____ *GSS*
_____ *MA*	_____ *MA*	_____ *MA*
_____ *Other System*	_____ *Other System*	_____ *Other System*

This section of the SSP must contain a brief (1-3 paragraphs) description of the function and purpose of the system and the organizational business processes supported, including functions and processing of data. Include major inputs/ outputs, users, and major business functions performed. If it is a GSS, include all applications supported, including functions and information processed.

1.6.1 System Environment and Special Considerations

Provide a (1-3 paragraphs) general technical description of the system. Discuss any environmental factors that raise special security concerns (e.g., internet connectivity, dial-up access) and document the physical location of the system. Provide a network diagram or schematics to help identify, define, and clarify the system boundaries for the system. Provide a description of the system and sub-applications and other software intra-dependencies.

NOTE: This section must provide standalone information regarding the operational environment within the scope of the SSP. Do not provide references to other documents without providing all the pertinent information within this section.

1.6.2 System Interconnection/Information Sharing

Describe any system interconnections and/or information sharing (inputs/ outputs) outside the scope of this plan. Show how the various components and sub-networks are connected and/or interconnected to any other system. Include information on the authorization for connections to other systems or the sharing of information. Document any written management authorizations with other agencies (e.g., Memorandum of Agreement [MOA], Memorandum of Understanding [MOU], Data Use Agreements) in this section.

1.6.3 Applicable Laws or Regulations Affecting the System

List any specific laws and regulations not documented in the CMS Master Plan that are applicable to the information processed by the system which establish specific requirements for confidentiality, integrity, availability, (CIA) auditability and accountability of information in the system.

1.6.4 General Description of Information Security Level

Determine the appropriate Information Security Level based on the CMS Standard in Appendix B - CMS Information Security Level Standards.

Business Partner Note: The security level will be provided by the CMS Business Owner.

Section 2. MANAGEMENT CONTROLS

Management controls focus on the management of the computer security system and the management of risk for a system. In the sub-sections below, describe the overall management controls that are currently implemented (i.e., in place) for the system. Each security control measure must be described in enough detail to determine if they are adequate.

2.1 Risk Assessment (RA) and Risk Management

The risk assessment must describe the methods used to assess the nature and level of risk to the system. State the risk assessment methodology used and describe if different from the CMS Risk Assessment Methodology. If the risk assessment is contained in a separate document, attach that document to the SSP, and provide a summary of that document here with a reference to the attachment.

Complete the following table for all of the system-specific vulnerabilities (excluding Low risk levels). The vulnerabilities included in the following table should map directly to the RA report. That is, Vulnerability 1 (V1) in the RA report should be identified as V1 in the table, V2 in the RA report should be identified as V2, etc.

RISK ASSESSMENT				RISK MANAGEMENT	
Vulnerability	Risk Level	Recommended Safeguard	Residual Risk	Status of Safeguard	Updated Risk

2.2 Review of Security Controls

If other types of security evaluations were conducted on the system during the past 12 months (e.g., GAO SAS-70, IG, Internal Revenue Service [IRS] audits), information about who performed the review, when the review was performed, the purpose of the review, a summary of general findings, actions taken as a result of the review, and a reference to the location of the full report and corrective action plans. Include a summary of the most recent self-assessment in this section.

2.3 Rules of Behavior (ROB)

The backside of the CMS form “Application for Access to CMS Computer Systems” contains the enterprise-wide ROB. Provide a definition of each type of user of the system (e.g., user, developer, sysadmin, DB admin) and a summary of the rules of behavior or “code of conduct” specific to your system for each type of user, including how often the system users are required to re-acknowledge the rules and how is this process documented. These ROB (e.g. password construction/maintenance, changing system data, searching databases, divulging information, working at home, dial-in access, connection to the Internet, assignment and limitation of system privileges) must include the consequences of non-compliance and must clearly state the exact behavior expected of each person. If the ROB are contained in a separate document, provide a summary of that document here with a reference for the responsible component.

2.4 Security in the SDLC

Identify how security was implemented into the life cycle phase(s). All legacy systems and systems developed by CMS through the Investment Planning Management Process (IPMP), need only refer to the CMS Master SSP. For all other systems, see Chapter 5 Figure 3, "SDLC and Security Lifecycle Phases and Associated Activities" for the SDLC requirements.

Section 3. OPERATIONAL CONTROLS

In the sub-sections below, describe the day-to-day procedures and mechanisms to protect operational systems. If this information is contained in a separate document, summarize the controls here and provide the document name/title, document control number (if applicable), document date, office responsible for maintaining the document (not a person's name), and location of the document (where it is available for review). Specify the document reference before providing the document summary.

3.1 Personnel Security Controls

Describe the personnel security controls for the system. It is important to note that the information in this section applies to all CMS personnel, contractor personnel and other external users. Personnel controls include individual accountability, least privilege, and separation of duties. All IT-related positions must be evaluated and sensitivity level assigned to the position description. Document if, when, and how personnel screening will be conducted.

3.2 Physical and Environmental Protection Controls

Describe the physical security and environmental protection controls for the system/application (e.g., access controls, fire safety factors, failure of supporting utilities, water sensors, structural collapse, plumbing, raised floor access, emergency exits). List the attributes of the physical protection afforded the area(s) where processing of the system/application takes place.

3.3 Production, Input/Output Controls

Describe the controls over the handling, processing, storage, and disposal of input and output data, media and any special production rules.

3.4 Incident Response Capability

Note: This section applies to GSS SSPs only.
Begin this section by describing any automated Intrusion Detection Systems (IDS) in place. Then, describe the following: the formal incident response capability and the capability to provide users with help when an incident occurs; the formal incident response capability available; and the procedures for recognizing, handling, and reporting incidents. Also document who responds to alerts/advisories and what preventative measures are in place (e.g., automated audit logs, penetration testing).

3.5 Contingency Planning and Disaster Recovery Planning

Describe the contingency plan(s) and disaster plan(s). Discuss arrangements and safeguards to ensure the alternate processing site will provide an adequate level of security, if applicable. Describe any documented backup procedures. Describe coverage of backup procedures and physical location of stored backups. Describe the generations of backups kept.

3.6 Hardware, Operating System, and System Software Maintenance Controls

In the sub-sections below, describe the security controls used to monitor the installation and updates to hardware, operating system software, and other system software to ensure that the hardware and software functions as expected and that a historical record is maintained of system changes.

3.6.1 Configuration Management (CM)

Note: This security control applies to GSS SSPs only. For MA's, reference the GSS(s) that support(s) the MA.
Describe the CM procedures for the system including; testing and/or approving system components prior to production, impact analyses to determine the effect of proposed changes on existing security controls and change identification, approval, and documentation.

3.6.2 Environmental System Software Management

Note: This security control applies to GSS SSPs only. For MA's, reference the GSS(s) that support(s) the MA.
Describe the controls used to: coordinate and control updates to the environmental system software, monitor the installation and updates of the software to ensure that it functions as expected and that a historical record is maintained of changes and policies for handling copyrighted software or shareware.

3.6.3 Application Software Management

Note: This security control applies to MA & "Other" Systems only.
Describe the CM version controls used to; coordinate and control updates to application software, monitor the installation and updates of the application to ensure that the software functions as expected and that a historical record is maintained of software changes.

3.7 Data Integrity/Validation Controls

Describe integrity controls for the systems to prevent/detect destruction or unauthorized data modification, including controls used to protect the information, operating system, application, and other system software (including security software) from accidental or malicious destruction or alteration.

3.8 Documentation

List the existing documentation that describe the system its components, operations, and use. Include the title, date, and the office responsible for maintaining the documentation (e.g., formal SDLC documents).

3.9 Security Awareness and Training (SAT)

Describe the system specific security training for all users who are involved with the management, use, or operation of the system. List the types and frequency of system specific training established, how the training will be conducted.

Section 4. TECHNICAL CONTROLS

In the sub-sections below, describe how the following technical controls have been implemented for the system. Discuss the logical controls in place to authorize or restrict the activities of users and information technology personnel within the system. If this information is contained in a separate document, summarize the controls here and provide the document name/title, document control number (if applicable), document date, office responsible for maintaining the document (not a person's name), and location of the document (where it is available for review). Specify the document reference before providing the document summary.

4.1 Identification and Authentication Controls

Describe user identification and authentication controls for the system, including mechanisms that provide the ability to verify users. If the system uses application specific passwords, describe in detail the characteristics of the passwords, (e.g., minimum & maximum length, character set limits/requirements, password aging.)

4.2 Authorization and Access Controls

Describe user authorization and access controls for the system. Be sure to include any specific system hardware or software features (e.g., Access Control Lists [ACL]) used to control access to the system resources by defining which users can access which resources. A description must be included indicating how users (in various roles) request and are approved for access to the system. Describe any system specific warning/notice banners. Provide a screen image of any system specific warning banners or notices of system criticality or data sensitivity.

4.3 Remote Users and Dial-up Controls

Describe remote users and dial-up access controls for the system. Describe the type of remote access (e.g., dialup, VPN, Internet) permitted and the functions that may be authorized for remote use (e.g., e-mail only, data retrieval only, full access).

4.4 Wide Area Networks (WAN) Controls

Describe WAN security controls for the system. If the system is running on a GSS that is connected to the Internet or other wide area network(s), discuss what additional hardware or technical controls have been installed and implemented to provide protection against unauthorized system penetration and other known Internet threats and vulnerabilities (e.g., VPN, Network Firewalls).

4.5 Public Access Controls

Describe the public access controls in place, including the access controls used to secure the system and information, if the system provides access to the public. Privacy statements and warnings must be described here. In addition, provide a screen image of any warning banners for systems that allow public access.

4.6 Test Scripts/Results

Describe the test scripts and results that were used to test the effectiveness of the security controls. Unavailable test scripts for legacy systems should be noted.

4.7 Audit Trails

Describe the auditing mechanism controls to allow management to conduct an independent review of recent activities. Include what is recorded, who reviews the audit trail, how often it is reviewed, and what procedures are employed for corrective actions as a result of a finding. Describe when audit trails are employed (e.g., on a given cycle, continuously, when an incident occurs, etc.). Describe the audit trail archive procedures, including how long they are kept, where they are stored, and what media type they are stored on.

Section 5. APPENDICES AND ATTACHMENTS

The following appendices represent documentation that may be developed and maintained as separate documents but must be included with the SSP for evaluation by the CIO or designee before accreditation. Maintaining these documents as appendices facilitates configuration management of all the related materials. These appendices can be updated without a recertification/reaccreditation if there is no change in the security profile.

Appendix A – Equipment List (primarily for GSSs only)
Appendix B – Software List
Appendix C – Glossary of Terms
Appendix D – Acronyms

For Glossary of Terms and Acronyms refer to http://cms.hhs.gov/it/security. Add only the terms that are referenced in the SSP and not found on the website.

Do not attach or include large documents with the SSP including Appendices. Instead, summarize the document in the appropriate SSP section; and provide the document name/title, document control number (if applicable), document date, office responsible for maintaining the document (not a person's name), and location of the document (where it is available for review).

APPENDIX B – CMS INFORMATION SECURITY LEVEL STANDARD[5]

The systems security efforts of the CMS IS Program are based on the sensitivity of data contained in all systems, and the operational criticality of the data processing capabilities of those systems. The most critical information assets are the data recorded in these assets, such as financial, Medicare, patient, and hospital records.

System Owners/Managers must determine the appropriate system security level based on the confidentiality, integrity and availability of the information, as well as its criticality to the agency's business mission. This is the basis for assessing the risks to CMS operations and assets and in selecting appropriate security controls and techniques.

CMS Standard for Information Security Levels establishes common criteria for security levels by information category. The first table defines the information security levels. The second table lists security levels for the various information categories. (Note: that mission critical information is its own category). In other words, the system owner locates his information category to find the appropriate system security level. In the cases where information of varying security levels are combined, the highest security level takes precedence. Where system availability or data integrity are of high importance, see the table footnote.

Information Security Levels

Security Level	Description	Explanation
Low	Moderately serious	Noticeable impact on an agency's missions, functions, image, or reputation. A breach of this security level would result in a negative outcome; or Would result in DAMAGE, requiring repairs, to an asset or resource.
Moderate	Very serious	Severe impairment to an agency's missions, functions, image, and reputation. The impact would place an agency at a significant disadvantage; or Would result in MAJOR damage, requiring extensive repairs to assets or resources.
High	Catastrophic	Complete loss of mission capability for an extended period; or Would result in the loss of MAJOR assets or resources and could pose a threat to human life.

Information Security Levels by Information Categories

Information Category	Explanation and Examples	System Security Level*
Investigation, intelligence-related, and security information (14 CFR PART 191.5(D))	Information related to investigations for law enforcement purposes; intelligence-related information that cannot be classified, but is subject to confidentiality and extra security controls. Includes security plans, contingency plans, emergency operations plans, incident reports, reports of investigations, risk or vulnerability assessments certification reports; does not include general plans, policies, or requirements.	High

5 Version 1.0 a*pproved as CMS standard by CTAB on September 27, 2002*

Mission-critical information	Information designated as critical to an agency mission, includes vital statistics information for emergency operations.	High
Life-critical information	Information critical to life-support systems (i.e., information where inaccuracy, loss, or alteration could result in loss of life).	High
Information about persons	Information related to personnel, medical, and similar data. Includes all information covered by the Privacy Act of 1974 (e.g., salary data, social security information, passwords, user identifiers (IDs), EEO, personnel profile (including home address and phone number), medical history, employment history (general and security clearance information), and arrest/criminal investigation history).	Moderate
Financial, budgetary, commercial, proprietary and trade secret information	Information related to financial information and applications, commercial information received in confidence, or trade secrets (i.e., proprietary, contract bidding information, sensitive information about patents, and information protected by the Cooperative Research and Development Agreement). Also included is information about payroll, automated decision making, procurement, inventory, other financially-related systems, and site operating and security expenditures.	Moderate
Internal administration	Information related to the internal administration of an agency. Includes personnel rules, bargaining positions, and advance information concerning procurement actions.	Moderate
Other Federal agency information	Information, the protection of which is required by statute, or which has come from another Federal agency and requires release approval by the originating agency.	Moderate
New technology or controlled scientific information	Information related to new technology; scientific information that is prohibited from disclosure to certain foreign governments or that may require an export license from the Department of State and/or the Department of Commerce.	Moderate
Operational information	Information that requires protection during operations; usually time-critical information.	Moderate
System configuration management information	Any information pertaining to the internal operations of a network or computer system, including but not limited to network and device addresses; system and protocol addressing schemes implemented at an agency; network management information protocols, community strings, network information packets, etc.; device and system passwords; device and system configuration information.	Moderate
Public information	Any information that is declared for public consumption by official authorities. This includes information contained in press releases approved by the Office of Public Affairs or other official sources. It also includes Information placed on public access world-wide-web (WWW) servers.	Low
Other sensitive information	Any information for which there is a management concern about its adequate protection, but which does not logically fall into any of the above categories. Use of this category should be rare.	Low

*This level is based on data sensitivity requirements for the information system. The low system security level may be increased to moderate (not to high) if the information system has significant integrity and/or availability requirements. The moderate level cannot be increased to high.

A system may be compartmentalized; such that a given data set or sub-process is more sensitive than other data sets or sub-processes. The appropriate System Owner/Manager and System Maintainer/Developer must assign the highest security level designation of any data set or sub-process within the system for the overall system security level designation. This practice supports the following:

- **Confidentiality.** The system contains information that requires protection from unauthorized disclosure.
- **Integrity.** The system contains information that must be protected from unauthorized, unanticipated, or unintentional modification, including the detection of such activities.
- **Availability**. The system contains information or provides services that must be available on a timely basis to meet business requirements or to avoid substantial losses.

System Owners/Managers and System Maintainers/Developers must ensure that their databases and the processing capabilities of their systems are accessed only by authorized users who fully use the required security level safeguards. The managers of compartmentalized systems must take special care to specify the appropriate level of security required when negotiating with other systems for services. The security level designation determines the minimum-security safeguards required to protect sensitive data and to ensure the operational continuity of critical data processing capabilities.

APPENDIX C – GLOSSARY of TERMS

See the *CMS Information Security Terms and Definitions* at http://cms.hhs.gov/it/security

APPENDIX D – LIST OF ACRONYMS

See the *CMS Information Security Acronyms* at http://cms.hhs.gov/it/security