Chief Information Officer
Office of Information Services
Centers for Medicare & Medicaid Services

CMS SYSTEM SECURITY PLAN (SSP) PROCEDURE

March 19, 2009

Version 1.0 - Final

Summary of Changes in SSP Procedure Version 1.0

1. This document replaces the *System Security Plans (SSP) Methodology*, dated October 28, 2002, version 3.0.
2. The CMS SSP Template was Appendix A to the *System Security Plans (SSP) Methodology document and as SSP Template*, v2.3 dated June 18, 2002. The *CMS SSP Procedure,* version 1.0 introduces the replacement to both of these documents. The *System Security Plans Template,* v3.0, dated March 09, 2009 is a separate document for Business Owners to complete to develop a SSP.
3. Global modifications were made to bring the SSP Procedure in line with current CMS policy and procedures contained within the CMS enterprise-wide Program documents.
4. Federal agencies must meet the minimum security requirements defined in FIPS 200 through the use of the security controls in NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*, which contains the management, operational and technical safeguards or countermeasures prescribed for an information system. The *SSP Methodology* identified sections 2, 3, and 4 to address Management, Operational, and Technical Controls. The *SSP Procedure* is based on NIST SP 800-53 and the security controls are organized into *families* and there are seventeen (17) security control families from NIST and an additional eighteenth family (E-authentication). Each family contains security controls related to the security functionality of the family. The security controls selected or planned must be documented in the SSP. It was further necessary to replace the *SSP Methodology* because the Business Risk and Technical Risk formerly identified in two separate documents have been combined into the *CMS Information Security Risk Assessment Procedure (IS RA).*

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This document replaces the Centers for Medicare & Medicaid Services (CMS) *System Security Plan (SSP) Methodology*, dated October 8, 2002. The *CMS System Security Plan (SSP) Procedure* presents a systematic approach for the SSP process, and the steps required to produce an SSP for systems that are part of a General Support System (GSS) or GSS subsystem, or a Major Application (MA) or MA individual application. This Procedure has been developed to provide the CMS Business Owners with the tools to determine, implement and document the current level of information security (IS) controls throughout the life-cycle of the system. System security planning is an essential function that is an iterative process within the life-cycle of a system and is used (with other security artifacts) to determine whether the system will be granted an authority to operate, i.e., accreditation. The Business Owner is responsible for ensuring that, based on the system security level, the IS controls within a system meet the required baseline security controls as defined in CMS IS policies and standards. The SSP documents the IS controls that protect the confidentiality, integrity and availability (CIA) of the system and its information in accordance with "Title III of the E-Government Act, entitled the Federal Information Security Management Act (FISMA)" and Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources," Appendix III, "Security of Federal Automated Information Resources,"

The *CMS SSP Procedure* provides the general roles and responsibilities that govern the implementation of the Business Owner's SSP as well as a life-cycle phase-by-phase description of the activities of which the Business Owner should be aware and perform at each phase of the life-cycle. In addition, steps and processes to document the system security planning functions performed by the Business Owner working with their System Developer/Maintainer and Information System Security Officers (ISSO) shall include the following:

- Describe Business Function / System Purpose and Description;
- On-going Data Collection;
- Identify and Document Current Security Controls; and
- Identify and Document Risks.

The *CMS SSP Procedure* provides instructions for completing an SSP and the Business Owner shall complete the *CMS SSP Template* to ensure an accurate identification, capture and communication of the system's current security posture and any business and technical risks that require mitigation. The SSP is an essential component of the CMS IS Program. This document provides an overview of the interfaces between the SSP and the following:

- *CMS Policy for the Information Security Program (PISP);*
- *CMS Information Security Acceptable Risk Safeguards (ARS) including the CMS Minimum Security Requirements(CMSR) [Low, Moderate, High];*
- *CMS Information Security (IS) Certification and Accreditation (C&A) Program Procedure;*
- *CMS System Security Level by Information Type;*
- *CMS Information Security Risk Assessment (IS RA) Procedure;* and
- *CMS System Security Plan Workbooks*

1. INTRODUCTION

1.1. OVERVIEW

The Centers for Medicare & Medicaid Services (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, as well as universal familiarity with data processing. Because new technology, too often is adopted before protective measures are developed, these factors have resulted in increased vulnerability of information and information systems. Without a corresponding growth in good information security (IS) 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' integrity and credibility.

The *CMS System Security Plan (SSP) Procedure*, hereafter known as "*The SSP Procedure*", covers all aspects of IS for information technology (IT) systems. 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 on behalf of CMS. In other words, any entity that processes information or performs IT processes on behalf of CMS, must have that system covered by an SSP. 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.

The SSP Procedure is used by those individuals responsible for IS at the system level and at the organization level. This document, which provides a specific format for an SSP and instructions on its content, should be used as a guide when creating SSPs. The implementation of these procedures as required by the CMS *Policy for the Information Security Program (PISP*) ensures a standardized development of SSPs and improves the security posture of the Agency.

The SSP Procedure is based on the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-18, Rev. 1; dated February 2006, *"Guide for Developing Security Plans for Information Technology Systems"*. Although the structure of these procedures and the NIST SP 800-18 are very similar, The *SSP Procedure* has been developed and tailored for use within CMS.

To manage a risk-based IS program, Business Owners are responsible for adhering to and implementing the policy and procedures contained with the following CMS enterprise-wide IS Program documents found at https://www.cms.hhs.gov/informationsecurity including but not limited to the following:

- *CMS Policy for the Information Security Program (PISP);*
- *CMS Information Security Acceptable Risk Safeguards (ARS) including the CMS Minimum Security Requirements(CMSR) [Low, Moderate, High];*
- *CMS Information Security (IS) Certification and Accreditation (C&A) Program Procedure;*
- *CMS System Security Level by Information Type; and*

- *CMS Information Security Risk Assessment (IS RA) Procedure*.

CMS requires each Business Owner to develop / update an SSP in response to each of the following events:

- New System;
- Major system modification;
- Expired accreditation (usually three years after the current accreditation of an operational system);
- Increase in security risks / exposure;
- Increase of overall system security level; and/or,
- Serious security violation(s) as described in the *CMS Information Security Incident Handling and Breach Notification Procedure*.

The CMS PISP requires updates to the SSP every three (3) years, at a minimum. However, it does require an annual review of the SSP for accuracy and the application of any updates resulting from that review. If during the annual review major changes arise the Chief Information Security Officer (CISO) should be apprised of fact and a re-accreditation will be required at that time.

The SSP documents the current level of security within the system, including reference to any applicable controls contained in the *CMS IS Master Plan* (hereafter referred to as the "Master Plan"). Although NIST allows for the documentation of *planned* controls, CMS requires that only the actual implemented controls are documented in the SSP. 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. Discussion of any planned changes in the implemented controls will be recorded in the IS RA as part of the recommended mitigations. Similarly, the SSP forms the primary reference documentation for testing and evaluation, whether by CMS, the Government Accountability Office (GAO), the Office of the Inspector General (OIG; or IG), or other oversight bodies.

1.2. OBJECTIVE OF THE CMS SSP PROCEDURE

The primary objective of *The SSP Procedure* is to provide IS guidance to CMS components and its partners in implementing an IS program that ensures compliance with regulations and standards. The SSP process must be followed to ensure continuity of operations and the confidentiality, integrity availability (CIA), auditability and accountability of CMS information and resources. Specifically, the CMS SSP Procedure provides instructions 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; and

- Create a framework for a secure IT environment that meets the requirements of Office of Management and Budget (OMB) A-130, Appendix III; Title III of the E-Government Act, entitled the Federal Information Security Management Act (FISMA); GAO, OIG, or other external or internal inspection, review or audit; and CMS operational requirements.

The SSP Procedure is intended to serve as a tool for the Business Owner, System Developer / Maintainer and SSP authors in determining the SSP requirements for a General Support System (GSS), a GSS sub-system, a Major Application (MA) or MA individual application. It is written to provide a specific format for developing an SSP and instructions on the content of the SSP. A template for the SSP titled 'System Security Plan (SSP) Template" can be found at:

http://www.cms.hhs.gov/informationsecurity/downloads/ssp_template.doc

1.3. PURPOSE

The primary goal of this procedure is to lay out the minimum requirements to describe the security protections for CMS'systems and to standardize the work of the System Developer/Maintainers and the Business Owners in creating SSPs.

The purpose of the SSP is to:

- Identify applicable laws and/or regulations affecting the system;
- Identify the rules of behavior associated with the system;
- Identify and provide details on the security controls related to the system within the pre-defined NIST control families and those for E-authentication, if applicable;
- Capture both High and Moderate level risks identified in the CMS IS RA;
- Identify how security is addressed in all levels of development; and
- Reaffirm information indicated within the corresponding system IS RA including, but not limited to:
  - Identify personnel responsible for oversight, development and the security of the system;
  - Identify the system operational status;
  - Identify the business process(es) associated with the system;
  - Identify the system environment;
  - Identify system interconnections; and
  - Identify the system security level.

All CMS employees and contractors are responsible for ensuring that CMS' information is protected adequately. OMB Circular A-130, Appendix III and FISMA prescribe the security controls that must be implemented to protect information resources. The security controls that OMB prescribes apply to all systems and are described in Table 1, OMB Circular A-130 Security Controls.

TABLE 1: OMB CIRCULAR A-130 SECURITY CONTROLS

Type of Control	Description
Assigning	Responsibility for security in each system is to be assigned in

Type of Control	Description
Responsibility	writing. The individual(s) responsible for a GSS must be knowledgeable in 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 and application life-cycles from pre-development and development through post development activities. Planning for security, at the on-set of the system and application life-cycles, 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 of all systems is to be performed at least every year. 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 proceed 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.

Under the FISMA of 2002, for a system in the requirements, design or implementation life-cycle phases, a defined set of security controls must be selected and incorporated into the system. Federal agencies must meet the minimum security requirements defined in FIPS 200 through the use of the security controls in NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*, which contains the management, operational and technical safeguards or countermeasures prescribed for an information system. The security controls are organized into *families* for ease of use in the control selection and specification process. There are seventeen (17) security control families from NIST and an additional eighteenth family (E-authentication). Each family contains security controls related to the security functionality of the family. The security controls selected or planned must be documented in the SSP. Table 2, Security Control Classes, Families and Identifiers describes the families and classes of the security controls. Note: although a control family may cover more than one function, the class most represented by the control is the designated class.

TABLE 2: SECURITY CONTROL CLASSES, FAMILIES AND IDENTIFIERS

IDENTIFIER	FAMILY	CLASS
AC	Access Control	Technical
AT	Awareness and Training	Operational
AU	Audit and Accountability	Technical
CA	Certification, Accreditation and Security Assessments	Management

IDENTIFIER	FAMILY	CLASS
CM	Configuration Management	Operational
CP	Contingency Planning	Operational
IA	Identification and Authentication	Technical
IR	Incident Response	Operational
MA	Maintenance	Operational
MP	Media Protection	Operational
PE	Physical and Environmental Protection	Operational
PL	Planning	Management
PS	Personnel Security	Operational
RA	Risk Assessment	Management
SA	System and Services Acquisition	Management
SC	System and Communications Protection	Technical
SI	System and Information Integrity	Operational
E-Authentication	E- Authentication	Technical

1.4. ROLES & RESPONSIBILITIES

The roles and responsibilities in this section are specific to information system security planning.

TABLE 3: ROLES AND RESPONSIBILITIES

Role	Responsibility
CHIEF INFORMATION OFFICER (CIO)	• Designated a Chief Information Security Officer (CISO) who shall carry out the CIO's responsibilities for system security planning; • Develops and maintain information security policies, procedures and control techniques to address system security planning; • Manages the identification, implementation and assessment of common security controls; • Ensures that personnel with significant responsibilities for SSPs are trained; • Assists senior agency officials with their responsibilities for SSPs, and identify and coordinate common security controls for the agency; and • Accredits systems based on certified SSPs and other supporting IS artifacts.
CHIEF INFORMATION SECURITY OFFICER (CISO)	• Carries out the CIO's responsibilities for system security planning; • Coordinates the review and acceptance of SSPs with Business Owners, Information System Security Officers (ISSO) and the authorizing official, i.e., at CMS - the CIO; • Coordinates the identification, implementation and assessment

Role	Responsibility
	of the common security controls; and • Possesses professional qualifications, including training and experience, required to review SSPs.
INFORMATION SYSTEM SECURITY OFFICER (ISSO) / SYSTEM SECURITY OFFICER (SSO)	• Assists the CISO in the identification, implementation and assessment of the common security controls; • Liaise with the Business Owner and the CISO to maintain consistent implementation of the SSP requirements; and • Assists in the development of the SSP package for accreditation by the CIO.
BUSINESS OWNER	• Develops and maintain the SSP and ensure that the system is deployed and operated according to the security requirements; • Ensures that system users and support personnel receive the requisite security training (e.g., instruction in rules of behavior); • Updates the SSP whenever a significant change occurs; • Assists in the identification, implementation and assessment of the common security controls; • Establishes the rules for appropriate use and protection of the subject data / information (Rules of Behavior); • Decides who has access to the information system and with what types of privileges or access rights; and • Submits the completed SSP package to the CISO for review and for accreditation by the CIO.
SYSTEM DEVELOPER / MAINTAINER	• Provides the technical support, and in practice, develops the SSP in coordination with Business Owners, the system administrator, the ISSO, the CISO and functional "end users"; • Implements the appropriate security controls for the assigned information system(s) as directed by the Business Owner; and • Assists in the identification and assessment of the common security controls where the information resides.

1.5. CMS SYSTEM SECURITY PLANS STRUCTURE

CMS has implemented a three-tiered hierarchical structure for its SSPs (see Figure 1). At the highest level is the Master Plan. The Master Plan follows the same format as all the SSPs and defines the enterprise-level common 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 Baltimore Data Center, training and awareness, etc. If the system operates within the boundaries of the common controls, the system SSP should not repeat the controls but just reference the Master Plan. For the areas covered by the Master Plan, it may not fully address the security controls as implemented for the individual system and, as such, each Business Owner is required to capture/document any departures in their security environment and controls in the SSP from the Master Plan.

Restated this means 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 the dependent systems will not have to be changed. This hierarchical structure also applies to any GSS, GSS sub-systems, MA, or MA individual application to which the system is related (see Figure 1). While each system/application requiring an SSP must develop a separately approved and accredited SSP, the common elements provided in the parent plan are inherited by the subordinate plans by establishing the relationship to a parent system and thus need only reference them. Any deviation from or exception to the inherited control must be reflected in the respective SSP. By following the hierarchical structure the Business Owner and System Developer/Maintainer is required to provide only that information and those protections that are unique to the particular system for which the SSP is being written.

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 affect another adversely is minimized. The GSS does not provide security beyond its own system protection levels, unless specifically requested to do so by the application managers. Simply implementing additional security controls does not ensure security. Security controls and products must be tested to ensure that they work and are being used correctly. Otherwise the security control may represent an additional area of vulnerability for the system.

In addition, all applications are required to have an individual SSP and IS RA unless the CISO specifically authorizes a combination into one SSP for the FISMA system family.

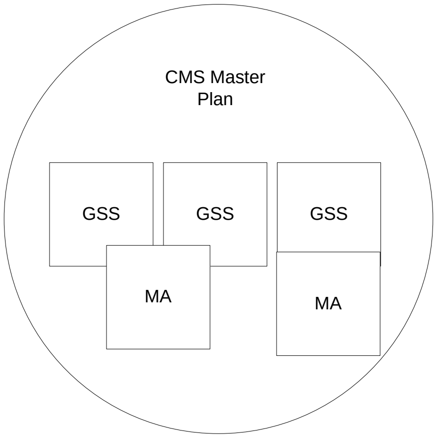

Figure 1: Three-Tier Hierarchical Structure of System Security Plans

Business Partner Note: CMS has established a Two-Tier Architecture with a GSS as the highest level (Figure 2). 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.

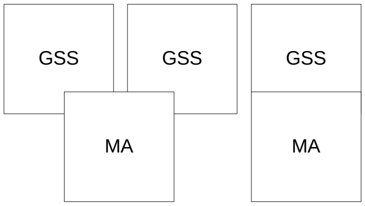

Figure 2: Two-Tier Hierarchical Structure of System Security Plans

The SSP should have the input of all involved managers and organization stakeholders. Table 4, SSP Properties describes the properties that personnel must keep in mind, when developing an SSP. The SSP shall be tailorable, scalable, predictable, understandable, relevant, repeatable, effective and evolvable.

TABLE 4: SSP PROPERTIES

Property	**Property Description**
Tailorable	The security process is applicable to any system regardless of the system status within the System Development Life-Cycle (SDLC) or shift in program strategy.
Scalable	The security process is applicable to systems differing in security requirements, size, complexity, connectivity and data policies.
Predictable	The security process is uniformly applicable to any system and minimizes personal opinion and subjectivity.
Understandable	The security process provides the participants with a consistent view of the security / compliance requirement of the system.
Relevant	The security process facilitates the identification of security requirements and solutions that are achievable (available, affordable and within the context of the development approach, Information Assurance (IA) strategies and mission needs).
Repeatable	The security process provides corresponding results when applied or re-applied to similar information systems.
Effective	The security process results in and maintains an accreditation for the target system.
Evolvable	The security process allows for the timely incorporation of lessons learned, and changes in security policy and technology.

1.6. SSP INTERFACES WITHIN CMS SECURITY ENVIRONMENT

The SSP Procedure is a set of processes and activities that must correlate with the development of a system. The SSP processes are integrated within CMS' life-cycle processes and procedures. A summary depiction of the interfaces within the CMS enterprise-wide IS environment is depicted below in Figure 3: CMS SSP Interfaces.

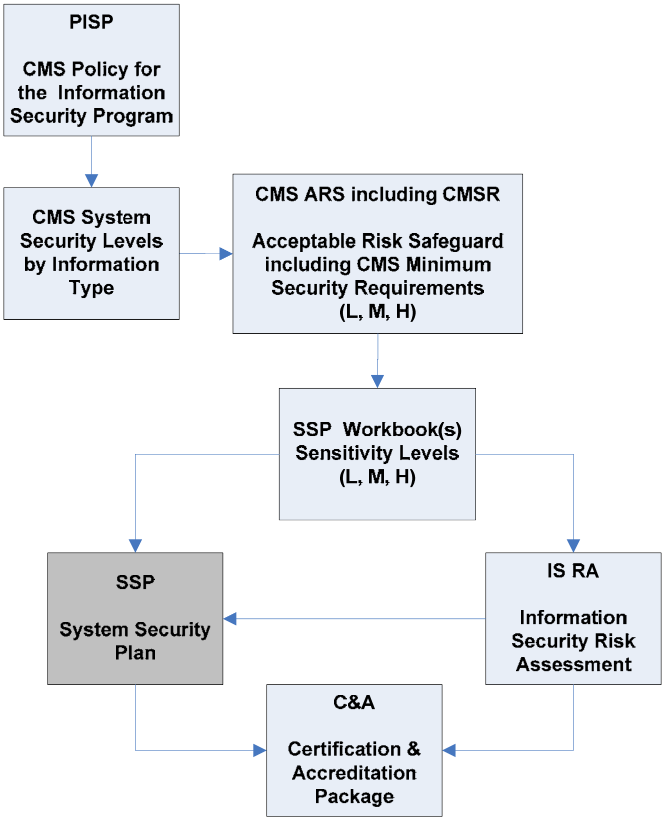
PISP
CMS Policy for the Information Security Program
CMS System Security Levels by Information Type
CMS ARS including CMSR
Acceptable Risk Safeguard including CMS Minimum Security Requirements (L, M, H)
SSP Workbook(s) Sensitivity Levels (L, M, H)
SSP
System Security Plan
IS RA
Information Security Risk Assessment
C&A
Certification & Accreditation Package

Figure 3: CMS SSP Interfaces

A summary description of the interfaces is as follows:

- CMS PISP – Establishes the policy for the CMS IS program and the ground rules under which CMS shall operate and safeguard its information and information systems to reduce the risk and minimize the effect of security incidents.
- CMS System Security Levels by Information Type – CMS has defined eleven (11) system security levels by information types. The CMS system security levels by information types is the first step taken by the Business Owner to define the system security levels. Once the level is established, the Business Owner will review the *CMS Information Security (IS) Acceptable Risk Safeguards (ARS)*.
- CMS IS ARS including the CMS Minimum Security Requirements (CMSR) [Low, Moderate, High] – Contains the minimum level of security controls that must be implemented to protect CMS' information and information systems. The Business Owners perform evaluations of all IS areas within the CMSR and determine the appropriate CMSRs for their systems. The Business Owner will document the expected minimum controls relative to the System Security Level of the system, as defined in the CMS IS ARS using the System Security Plan Workbook.
- System Security Plan Workbook(s) – The workbooks provide the Business Owner with a list of security controls that represent the minimum required controls to be implemented

based on the system security level (Low, Moderate, and High). The Business Owner will also utilize the security control workbooks to support development of the SSP and IS RA.

- IS RA – The Business Owner must document and certify that the incorporated security / internal controls are in place in the SSP. The risks and any mitigations must be documented in the IS RA. The Business Owner will include the IS RA as part of the Certification & Accreditation (C&A) package to support system certification and accreditation.
- SSP – The SSP contains a detailed description of IS controls that are in place for the system to ensure the system's CIA. The Business Owner will include the SSP as part of the C&A package to support system certification and accreditation.
- C&A – The C&A package contains the necessary documentation to demonstrate and to validate that appropriate security controls were implemented throughout the development of the system and exist to safeguard the system. The Business Owner will prepare the C&A package for the accreditation decision-maker to evaluate the system for certification and accreditation. (See *CMS Information Security (IS) Certification and Accreditation (C&A) Program Procedure f*or specifics).

2. SSP WITHIN THE CMS LIFE-CYCLE

The SSP should be developed, referenced and revised as the given system progresses through the CMS Integrated IT Investment & System Lifecycle Framework ("FRAMEWORK") located at:

http://www.cms.hhs.gov/SystemLifecycleFramework

The goal of CMS' "Framework" is to provide a structure for managing a system throughout its life-cycle from Initiation through Disposition including the incorporation of the appropriate protections of the information and the information system. However, an SSP is not simply a paper exercise 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.

A properly developed and maintained SSP is invaluable as it allows the organization to understand and monitor the effectiveness of the security controls. This procedure describes the steps necessary to produce a SSP, which incorporates information from the IS RA and is reviewed during the CMS IS C&A process. The SSP process supports CMS' enterprise security model by providing a foundation for the evaluation of system-related security controls. Appendix A, *SSP Template Instructions* includes directions on how to complete the SSPs. In addition, the actual SSP Template to be completed for all CMS systems can be found at:

http://www.cms.hhs.gov/informationsecurity/downloads/ssp_template.doc

CMS business partners should review the "Framework" to assist them in describing in their respective SSPs how their corporate life-cycle process / methodology implements IS. The CMS "Framework" can be found using the following URL:

http://www.cms.hhs.gov/SystemLife-cycleFramework/01_overview.asp

The CMS SSP Process is initiated during Requirements Analysis within the "Framework" or from a C&A perspective in the Initiation Phase of the C&A process. Figure 4 below depicts the CMS life-cycle phases and related SSP activities followed by the detailed description.

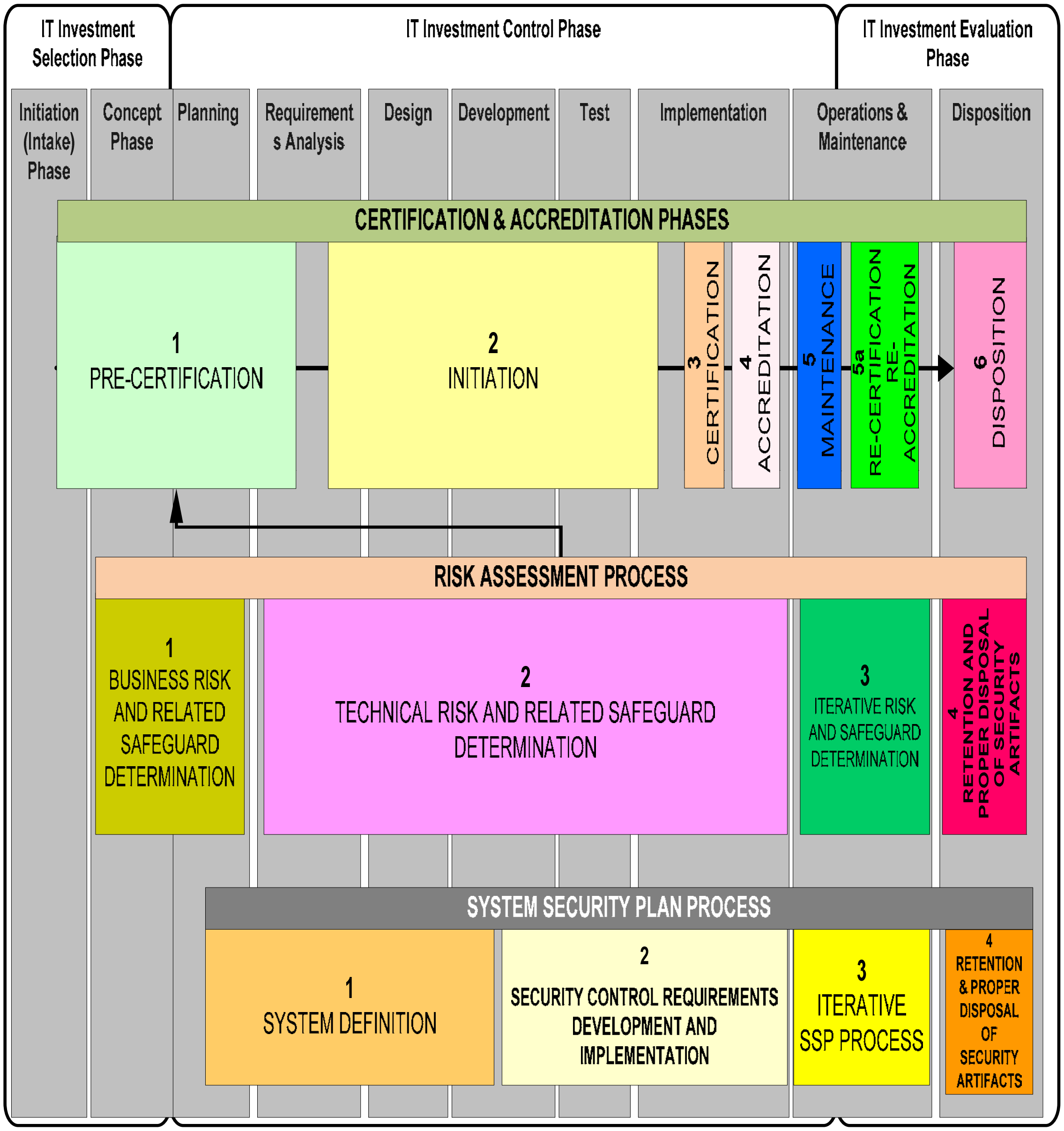
IT Investment Selection Phase
IT Investment Control Phase
IT Investment Evaluation Phase
Initiation (Intake) Phase
Concept Phase
Planning
Requirements Analysis
Design
Development
Test
Implementation
Operations & Maintenance
Disposition
CERTIFICATION & ACCREDITATION PHASES
1 PRE-CERTIFICATION
2 INITIATION
3 CERTIFICATION
4 ACCREDITATION
5 MAINTENANCE
5a RE-CERTIFICATION RE-ACCREDITATION
6 DISPOSITION
RISK ASSESSMENT PROCESS
1 BUSINESS RISK AND RELATED SAFEGUARD DETERMINATION
2 TECHNICAL RISK AND RELATED SAFEGUARD DETERMINATION
3 ITERATIVE RISK AND SAFEGUARD DETERMINATION
4 RETENTION AND PROPER DISPOSAL OF SECURITY ARTIFACTS
SYSTEM SECURITY PLAN PROCESS
1 SYSTEM DEFINITION
2 SECURITY CONTROL REQUIREMENTS DEVELOPMENT AND IMPLEMENTATION
3 ITERATIVE SSP PROCESS
4 RETENTION & PROPER DISPOSAL OF SECURITY ARTIFACTS

Figure 4: SSP Processes in the CMS Framework

2.1. PHASE 1 - INITIATION (INTAKE)

During this phase the Business Owner works with the CMS CISO to determine if the system is either a GSS or a MA and by what FISMA system family it will be categorized. CMS has already established a number of FISMA system family categories for GSSs and MAs. In order to ensure continuity with the already identified inventory of systems, the OIS, Enterprise Architecture and Strategy Group (EASG) should be contacted for appropriate designation. Once the Business Owner has obtained this designation, the identification of the System Security Level by Information Type, which contains eleven (11) types, is determined. Upon establishing the level, the Business Owner will review the CMS PISP and CMS IS ARS for the level controls that must be employed in the system.

2.2. PHASE 2 - CONCEPT

At this phase of the life-cycle, the Business Owner will begin to identify business risks and the initial draft of the IS RA is developed. The business risks during this phase are defined as the vulnerabilities and threats that could be exploited and result in the loss of business functionality. The risks identified at this stage are documented within the IS RA and identified controls will be included within the appropriate sections of the SSP, which is initiated in Phase 4 Requirements Analysis of the Framework.

2.3. PHASE 3 - PLANNING

The Business Owner reviews the *CMS IS ARS*, which contains the minimum threshold for security controls based on the system security level that must be implemented to protect CMS' information and information systems. The Business Owner performs an evaluation of all IS areas within the CMS IS ARS and determines the appropriateness of the families for their system. The Business Owner will identify the expected minimum controls relative to the sensitivity level of the system, as defined in the CMS IS ARS using the SSP Workbook. Additional identified risks are used to support the development of the system requirements, including security.

The Business Owner will review the applicable system security level determination from the Concept Phase (Low, Moderate, or High) to select and initiate population of the SSP Workbook The Business Owner should incorporate the appropriate SSP Workbook into other high-level planning documents.

2.4. PHASE 4 - REQUIREMENTS ANALYSIS

The Business Owner in collaboration with the System Developer / Maintainer is responsible for the initial development of the SSP during this phase in concert with the continued development of the IS RA. Substantive development of both documents begins based on the security controls in the CMS PISP and in the CMS IS ARS and utilizing the appropriate SSP Workbook. These represent the minimum required security controls, which, if not properly addressed, will result in most of the system risks. Any business risks identified in the Phase 2: Concept or Phase 3: Planning are carried forward into the IS RA and the SSP.

The initial IS RA, which identifies business risks in the Concept Phase of the Framework, serves as the foundation for the SSP. As the System Developer/Maintainer defines the requirements for the system, 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 CMS Baltimore Data Center), or operational practices (e.g., awareness and training). Extent of the initiation of the SSP is based on available information at the on-set of the life-cycle process.

2.5. PHASE 5 - DESIGN

The SSP is updated as needed during this phase. The SSP contains the detailed descriptions of controls that are in place for the system to ensure its CIA. The IS RA is also updated during this phase to account for any risks, vulnerabilities and safeguards that have been identified or changed.

Although these procedures address the SSP, the Business Owner needs to be aware of the synergetic relationship with the IS RA. While the SSP provides the detailed descriptions of all the implemented controls required by the CMS PISP / CMS IS ARS categories, to minimize these risks, the IS RA must detail the threats, vulnerabilities and risks affecting the system. The Business Owner shall refer to the CMS IS RA Procedure for the specifics on completing an IS RA.

The Business Owner is responsible for ensuring that the planned (that will be in place by implementation) or existing security controls are fully documented within the SSP. (Note: During the design phase, planned security controls can be incorporated within the SSP only if they are expected to be fully implemented prior to accreditation . The Final SSP submitted in the C&A package for accreditation should include only the in-place controls). The SSP also provides a complete description of the information system and its interconnections.

By the end of the design phase the SSP must be functional. Changes must continue to be made as the system matures and technology changes.

2.6. PHASE 6 - DEVELOPMENT

The SSP is further updated during this phase to ensure that security controls described in the SSP during design phase are actually implemented (Note: At system deployment, the planned controls documented in the design phase that were not implemented should to be deleted from the SSP. Only the security controls implemented should be described in the SSP). SSPs for information systems currently in operation may call for the development of additional security controls to supplement the controls already in place or the modification of selected controls that are deemed less than effective.

The SSP should include information gathered from the various other documents required by CMS' IS program such as the configuration management plan, contingency plan, incident response plan, security awareness and training plan, rules of behavior, risk assessment, security test and evaluation results, interconnection agreements, security authorizations/accreditations, and plan of action and milestones (POA&M). The security control workbooks can be used as a tool to collect the information and then feed it into the SSP

The IS RA is also updated in this phase to account for any risks, vulnerabilities and safeguards that have been identified or changed as the development process progresses.

2.7. PHASE 7 - TEST

The Business Owner shall identify an independent organization to conduct a Security Test and Evaluation (ST&E) based on the SSP and the IS RA[1]. The ST&E is a technique that is used to validate that the documented controls are employed as described in the SSP and to identify any additional system vulnerabilities as part of the risk management process. It includes the development and execution of a test plan (e.g., test script, test procedures and expected test results as defined in the *CMS IS Assessment Procedure*. The purpose of system security testing is to test the effectiveness of the security controls of an IT system documented within the SSP as they have been applied in an operational environment. The objective is to ensure that the applied controls operate as defined, meet the approved security specification for the software and hardware, and implement the organization's security requirement. As necessary, the Business Owner shall identify corrective actions and report the results according to the *CMS Reporting Procedure for Information Security (IS) Assessments* and the *CMS Information Security (IS) Plan of Action and Milestone (POA&M) Guidelines*.

2.8. PHASE 8 - IMPLEMENTATION

The Business Owner ensures that the functionality of the security controls are verified, validated and described properly in the SSP and IS RA. The SSP is finalized along with the IS RA and becomes input to the C&A Package. All the documentation required to form a part of the C&A package can be found within the C&A package located at:

http://www.cms.hhs.gov/informationsecurity/downloads/CA_template.doc.

The C&A of the system occurs as part of the Implementation Phase. The Business Owner may continue to update the SSP and the IS RA until the C&A process begins. The C&A package must contain the most current SSP and IS RA information for the system. The Business Owner will present the C&A package to the CIO through the CISO for accreditation according to the *CMS IS C&A Program Procedure*. The CIO can provide a signed system authority to operate, i.e., accreditation, a conditional authority to operate, or deny operation of the system until certain corrective actions are taken.

[1] The Business Owner shall wherever possible, employ the OIS contracts for an ST&E. The CISO must approve if other arrangements have been made for an independent contractor to conduct the ST&E to verify that all CMS ST&E requirements will be met.

2.9. PHASE 9 - OPERATIONS AND MAINTENANCE

During this phase of the Framework, the SSP must be the most complete and change only with modifications to systems, risks or policy. As part of the risk management activities, the SSP must be reviewed every three hundred and sixty five (365) days and the review log must completed. The Business Owner shall update the SSP and IS RA on an "as needed" basis. Any changes to the IS RA may necessitate a change within the security controls documented within the SSP or vice versa. A system re-certification and re-accreditation is conducted at a minimum every three (3) years. Also re-certification and re-accreditation occurs when there is a major modification to the system, when the system security level has changed, or a major security control has been compromised. The Business Owner shall conduct annual FISMA assessments (FA) as well as annual Contingency Plan (CP) testing every three hundred and sixty five (365) days. All identified risks or findings must be used to update the SSP and the IS RA.

2.10. PHASE 10 - DISPOSITION PHASE

The Business Owner in this phase must archive the SSP, and all accredited versions, in accordance with Federal records retention and archiving requirements. During this phase, the system and components are also archived and maintained for three (3) years after system is declared retired. The maintenance requirement is for IS records purposes only as defined by National Archives and Records Administration (NARA) Schedule 24 and is not intended to supersede or circumvent other established requirements for maintaining records.

3. DEVELOPMENT OF THE SSP (SSP PROCESS)

The Business Owner shall review and utilize the steps and processes defined in this section to develop an SSP. In addition the Business Owner shall utilize the SSP Template to complete an SSP for their respective GSS, GSS subsystem, MA and MA individual application. The SSP process includes tasks and milestones associated for each step.

3.1. SYSTEM DEFINITION PROCESS

The System Definition process is the first process implemented. The need for a system is expressed and the purpose of the system is documented. This information is supported further by determining the system boundaries, system category (i.e., GSS, GSS sub-system, MA, individual application within an MA) and System Security Level (High, Moderate or Low) based on the information type identified during the IT Investment Selection Phase.

3.1.1. DETERMINE THE SYSTEM BOUNDARIES

The first step in initiating the SSP 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 an SSP. Each component of the system must:

- Be under the same direct or indirect management control (i.e., one FISMA family Business Owner even though the applications supporting the MA are not necessarily under the same direct management control); and
- Have the same general business function(s) or business objective(s).

All components of a system do not need to be connected physically.
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; and
- 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 necessary to use plans that are identical except for those areas of difference. This approach provides coherence and consistent levels of protection for similar systems.

3.1.2. DETERMINE SYSTEM CATEGORY

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

- GSS, (e.g., an infrastructure component such as the CMS Baltimore Data Center, Quality Net (Qnet), etc.);
- GSS sub-system (e.g., mainframe, Enterprise User Interface (EUA), etc.);
- MA, (e.g., Human Resources Management System (HRMS), Administrative Finance System (AFS), etc.); and
- MA individual application (e.g., CMS Human Resources Information System (CHRIS) under HRMS, Budget Under Control System (BUCS) under AFS, etc.),

CMS has already established a number of FISMA system family categories for a GSS and MA. In order to ensure continuity with the already identified inventory of systems, the Office of Information Services (OIS), Enterprise Architecture and Strategy Group (EASG) must be contacted for appropriate designation.

3.1.3. SYSTEM SECURITY LEVEL ASSESSMENT

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 information systems. System security level designations are used to define the requirements for all CMS information systems to protect information assets. Some of CMS' most critical information assets are the data residing within a system, such as financial, Medicare enrollment information, personal health records and identifiable personal data. Business Owners must determine the appropriate system security level based on the CIA of the information, as well as its criticality to the agency's business mission. This determination provides the basis for assessing the risks to CMS operations and assets in selecting appropriate security controls and techniques.

The CMS System Security Level by Information Type documents the categories of information that support the system and classify the system security level as Low, Moderate or High for the Business Owners. *The CMS System Security Level by Information Type* document can be downloaded from this link:

http://www.cms.hhs.gov/informationSecurity/Downloads/ssl.pdf

3.1.4. INCORPORATING RISK ASSESSMENT INFORMATION

Beginning before and in conjunction with the SSP, an IS RA must be performed iteratively throughout the life-cycle phases. The initial RA which identifies business risks in the Concept Phase of the Framework, serves as the foundation for the SSP. System planners define the high-level requirements for the system and security requirements must considered 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 CMS Baltimore Data Center), or operational practices (e.g., awareness and training). Extent of the initiation of the SSP is based on available information at the onset of the life-cycle process.

3.1.5. SECURITY CONTROL WORKBOOK

Business Owners are strongly encouraged to complete the SSP Workbook. The Security Control Workbooks provide the Business Owner with a list of security controls that represent the minimum controls required for the system based on the system security level. These controls are based on the CMS IS ARS. Commensurate with the CMS IS ARS, four (4) SSP Workbooks have been developed that correspond to the three (3) system sensitivity levels, i.e., Low, Moderate and High and one for E-authentication. The level of sensitivity of the system is driven by the guidance provided in the CMS System Security Level Standard. The Workbooks should be completed thoroughly, and in their entirety, as a part of the overall IS effort. For new systems, the appropriate Security Control Workbook should be selected once the system security level is determined and completed during the SSP process . For existing systems, the Security Control Workbook should be completed when significant changes are made to a system and its security controls and/or when there is a change in the systems security level, which requires a system to be re-accredited. These Security Control Workbooks will prove to be an invaluable resource that can be utilized during audits in developing security-related documentation (IS RA and SSP) and be referenced when there is a change in system-related personnel.

The information contained within the Workbooks is used to complete the SSP. When applicable, it is acceptable for the author to copy and paste the information documented within the row titled “Security Controls Detail and Comment” from the Workbook for each family into the SSP template - Section 2 titled “Security Controls Detail and Comment”. The section includes the implementation of security controls for each of the control families and CMS E-authentication standards.

Note - The details and comments contained within the SSP template will be considered the information of record. Therefore, great care must be taken to ensure that the SSP template contains accurate and up-to-date information

TASK 1: INITIATION OF THE SSP

The objective of this task is to:

- Determine system boundaries;
- Determine system category;
- Prepare initial IS RA; and
- Prepare a draft SSP.

Task 1 Activities:

1. Determine system boundaries.
2. Determine system category.
3. Identify the System Security Level by information type.
4. Initiate IS RA process.
5. Define security requirements and operational practices utilizing the appropriate workbook.
6. Produce draft SSP and IS RA.

The Business Owner and the System Developer/Maintainer shall ensure that the following activities take place during this task:

- Assess the information processed by the system.
- Define the security requirements concurrent with the system requirements utilizing the Security Control Workbook for the appropriate System Security Level.

System Documentation Process Milestones:

- All system identification information has been captured.
- All risks identified in the IS RA have been documented into the SSP

3.2. SECURITY CONTROL REQUIREMENTS AND IMPLEMENTATION PROCESS

During the Development and Implementation Phase of the Framework, the system is designed, purchased, programmed, developed or otherwise constructed. During this phase, the SSP must be functional as the phase approaches its end. Changes must continue to be made as the system matures and technology changes.

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. The Business Owner and System Developer/Maintainer, as a management control, perform system certification. The CMS CIO or his/her designee accredits the system based on the recommendation of the CISO. Additionally, if new controls are added to the application or GSS, 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 SSP must be complete and functional.

TASK 2: COMPLETION OF THE SSP

The objectives of this task are:

- Address all security-related required controls and issues
- Document the baseline configuration of the system
- Acceptance testing of controls
- Updating and finalization of the SSP

Task 2 Activities:

1. Verify and finalize the identification of security requirements
2. Update security requirements to mitigate new risks/threats.
3. Verify the development of security controls, with associated testing procedures prior to system procurement/development.
4. Establish that the IS RA reflects additional risks identified during development, indicate risks mitigated by development, and that security plan addresses risk management.
5. Update the SSP.

The Business Owner and System Developer/Maintainer shall ensure that the following activities take place during this task:

- Verify and finalize the comprehensive identification of security requirements during system design;
- Ensure that solicitation documents and/or development agreements permit the update of security requirements designed to mitigate new risks/threats;
- Verify and finalize the development and implementation of appropriate security controls;
- Establish that the IS RA reflects additional risks identified during development, indicate risks mitigated by development, and that SSP addresses risk management; and
- Update the SSP to reflect all of the aforementioned bullet points.

Security controls must be implemented based on those prescribed by OMB Circular A-130, Appendix III, NIST SP 800-53 and CMS specific requirements.

TASK 3: ASSEMBLY OF THE SSP PACKAGE

The objective of this task is to:

- Organize all SSP information as part of one comprehensive, and organized C&A package.
- Create and electron version of the package on CD.
- Submission of C&A package to the CISO for approval by the CIO.

Task 3 Activities:

1. The SSP package is prepared for certification.
2. All SSP documentation is presented in a three ring binder as part of the C&A package.
3. An electronic copy of the C&A package is created on CD.
4. The C&A package is submitted by the Business Owner for Accreditation to the CISO for approval by the CIO.

The Business Owner and System Developer/Maintainer shall ensure that the following activities take place during this task:

- The SSP is prepared for certification by the Business Owner, System Developer/Maintainer and the ISSO

- The SSP and all related SSP documentation is assembled. presented in a three-ring binder as part of the C&A package;
- The electronic copy of the C&A package is provided on CD; and
- The C&A package is submitted by the Business Owner to the CISO for accreditation by the CIO.

Development Phase Milestones:
- Completion of SSP.
- Assembly of C&A package

3.3. ITERATIVE SSP PROCESS

During this Operations and Maintenance Phase of the Framework, the system is operational and functioning. If the system undergoes modifications, any changes to security activities must be documented in the SSP. These changes include level of risk, management of the risk, and mitigation and/or elimination of existing risks. In the SSP, security operations and administration, operational assurance and audits and monitoring must be described. During this phase of the Framework the SSP must be the most complete and only change with modifications in systems or policy.

TASK 4: REVIEW & UPDATE THE SSP

The objective of this task is to update the SSP to reflect any system modifications and/or changes to security activities.

The Business Owner and/or System Developer/Maintainer shall ensure that the following activities should take place during this task:

Task 4 Activities:
Update SSP to reflect:
- Changes related to risk level, management, and mitigation of risks;
- Changes to the system;
- Changes in C&A status; and
- Changes in the descriptions related to security operations, administration, and assurance.
- If needed, C&A package for re-accreditation

- Update the SSP, as necessary, to reflect changes relative to level of risk, management of risk, mitigation and/or elimination of existing risks;
- Update the SSP, as necessary, to reflect changes to system architecture, system status, addition or deletion of system interconnections, change in system scope, and change in C&A status;
- Modify the SSP to include changes in the descriptions relative to security operations and administration, operational assurance and audits;

If significant changes are made to a system and its security controls and/or when there is a change in the systems security level, submit a re- accreditation package to the CISO for approval by the CIO.

***The CMS PISP requires updates to the SSP every three (3) years, at a minimum. However, it does require an annual review of the SSP for accuracy and the application of any updates resulting from that review. If during the annual review major changes arise the Chief**

Information Security Officer (CISO) should be apprised of fact and a re-accreditation will be required at that time. Periodic and required annual (within three hundred and sixty five (365) days) reviews provide assurance that management, operations, personnel and technical controls are functioning effectively, providing adequate levels of protection.

3.4. RETENTION AND PROPER DISPOSAL OF SECURITY ARTIFACTS PROCESS

During the disposition phase of the Framework, when the system is at the completion of its utilization, the Business Owner shall be responsible for ensuring the disposition of information, hardware and software. Before final destruction of the SSP, verification of any federal records as defined by the NARA retention period requirements must be investigated. Retention of the security artifacts used to support the C&A of a system must be retained for three (3) years following the expiration of the accreditation. However, depending on the type of data captured in these documents, there may be more stringent requirements by NARA. At the completion of a systems life-cycle (disposal of a system), the SSP, including every accredited version, must be archived in accordance with Federal records archiving requirements.

TASK 5: SYSTEM DECOMMISSION

The objective of this task is to archive all accredited versions of the SSP.
The Business Owner and/or System Developer/Maintainer shall ensure that the following activities should take place during this task is to archive the SSP, and all accredited versions, in accordance with Federal records retention and archiving requirements.

Task 5 Activities:
Archive all accredited versions of the SSP.

Post-Development Phase Milestones:

- Updated SSP
- Archived SSP, as appropriate

APPENDIX A: SSP TEMPLATE INSTRUCTIONS

Appendix A provides the detailed instructions for the Business Owner in completing the SSP using the SSP template. Initially, the Business Owner shall perform system identification by documenting the system name, related information and the responsible organization. Developed chronologically prior to the SSP, the IS RA serves as its foundation. However, given the amount of shared information, a skeleton SSP may be developed during the development of the IS RA. The author can update the SSP skeleton to reflect the following information contained in the IS RA:

- System Identification;
- System Operational Status;
- Description of the Business Process;
- System Interconnections;
- System Security Level; and
- Security Controls identified during development of the IS RA.

Additionally, the author shall include information not addressed within the IS RA:

- Applicable Laws or Regulations;
- Rules of Behavior; and
- Planning for Security in the SDLC.

Once the IS RA is finalized, Section 2.14 of the SSP template is updated to reflect Risk Assessment and Risk Management data elements as they appear in the IS RA Risks and Safeguards table (Section 3.0). It is important to note that section 2.14 of the SSP should only address those risks that are Moderate or High in nature.

The Business Owner, System Developer/Maintainer or author shall also provide details and comments pertaining to the security controls related to the eighteen (18) control families identified in Section 3.0 of the SSP template. If a SSP Workbook was completed during development of the IS RA, detail and comment information can be transferred to the corresponding control family section within the SSP. If a SSP Workbook was not completed, the Business Owner, System Developer/Maintainer or author is **strongly encouraged** to complete the workbook during development of the SSP. The circumvention of the use of the SSP Workbooks could result in a delay in the accreditation of the system since the workbooks shall serve as a record of the analysis of each required control.

The security of a system may degrade over time as the technology changes, or the system evolves, or changes occur to authorizing legislation or requirements, or people and procedures change. Periodic and required annual (within three hundred and sixty five (365) days) reviews provide assurance that management, operations, personnel and technical controls are functioning effectively, providing adequate levels of protection. The SSP is updated to reflect any appropriate changes in the security environment throughout the life-cycle.

All CMS information systems must undergo a ST&E, which is a third-party process conducted by an independent evaluator to assess the management, operational and technical controls. Periodic reviews are required for FISMA (section 3544(b) (5)) compliance and shall be conducted on a regular basis depending on risk and as defined by CMS IS ARS but no less then every three hundred and sixty five (365) days

FISMA does not require the annual assessment to include all security controls employed in an organizational information system. However, all security controls must be assessed over a three (3) year period. The Business Owner should test one-third of the security controls in any given annual assessment. If annual testing is performed by an independent evaluator, and over a three (3) year period covers all the management, technical and operational controls, the results of the annual assessment may be utilized as part of the ST&E.

A completed 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).

Instructions on how to complete the templates have been developed for each section within the template and shall be used for all sensitivity levels.

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 procedure, 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.

SYSTEM IDENTIFICATION

Use Section 2 from the IS RA as the foundation for this section "System Identification". Additional sub-sections not included within the IS RA also form a part of System Identification and these shall be addressed in accordance with the instructions provided. Any of the following sections not included within the IS RA shall be added as appropriate.

SYSTEM NAME AND TITLE

Provide the system identifier, which include the official name and/or title of system, including acronym and system of records (SOR) number, the Financial Management Investment Board (FMIB) number and the system type.

Instruction:
Provide the following:

- Official name and/or title of system,
- System acronym,
- SOR number,
- FMIB number, and
- Type of system.

SOR Number
SOR number can be obtained from the CMS Privacy Officer and must remain the same throughout the life of the system and be retained in audit logs related to system use. Assignment of an SOR number supports CMS's ability to collect CMS information and security metrics

specific to the system as well as facilitate complete traceability to all requirements related to system implementation and performance.

FMIB Number

During the "Framework" Implementation Phase, the investment is reviewed by the Information Technology Investment Review Board (ITIRB) / Financial Management Investment Board (FMIB). Approved investments are subsequently assigned an FMIB number. The FMIB number facilitates complete traceability to ensure continued viability of the investment assessed by compliance with established scope, budget, schedule and performance measures.

System Type

For CMS systems, check one box in the template to indicate whether the system is a MA, MA individual application, GSS or GSS sub-system. If the system contains minor sub-applications, describe them in the General Description / Purpose section of the plan.

Note: For non-CMS Baltimore Data Center hosted systems / applications, more than one system type can be checked. For any MA or MA application supported by a GSS, which is not listed as one of the CMS GSS System Families, the Business Owner and/or System Developer/Maintainer, has the option of combining the GSS and MA (or MA individual application). That is the IS RA requirements can be combined into one IS RA and the GSS and MA (or MA individual application) SSP requirements into one SSP. This same option is available to the External Business Partners (e.g., MACs, DMACs, etc.). Check the appropriate boxes.

Document if the System is a GSS or a GSS sub-system

The Business Owner obtains from the IS RA the designation of the system and documents within the SSP if the system in a GSS; GSS sub-system / MA or MA individual application.

RESPONSIBLE ORGANIZATION

Provide the contact information for the **CMS** organization responsible for the system. A designated responsible organization must be identified in the SSP for each system. The organization is responsible for coordinating SDLC activities specific to the system. CMS must be organization represented in this section.

Instruction:
Identify the responsible **CMS** organization for the system.

The SSP should include the following contact information:

- Name of Organization;
- Address;
- City, State, Zip;
- Contract Number; and
- Contract Name.

In addition to the CMS responsible organization, contractors and other non-CMS partners, can document their company specific information in another table that must be added below the table that documents the CMS information. However, this is optional.

DESIGNATED CONTACTS

Indicate the names of other key contact personnel who can address inquiries regarding system characteristics and operation. Required contacts include, but are not limited to, Business Owner, System Developer/Maintainer, SSP author, etc. The SSP should include the following contact information for each of the other designated contacts:
Name;

- Title;
- Organization;
- Address;
- Mail stop;
- City, State, Zip;
- E-mail;
- Telephone; and
- Contractor contact information (if applicable).

Instruction:
Identify additional personnel that can address system related inquiries. Provide contact information for each.

The Business Owner is a CMS Group Level or higher and the contact information for the System Developer/Maintainer must be CMS Division Level for the component performing the function or the component that has contracted out the function.

Other non-CMS partners can document their company specific information in another table that must be added below the table that documents the CMS information. However, this is optional.

ASSIGNMENT OF SECURITY RESPONSBILITY

Instruction:
Identify two (2) different security contacts.

This section requires two (2) different security contacts — one (1) primary security contact and one (1) different emergency contact. A CMS individual responsible for security shall be identified as the primary contact. The emergency contact should know how to contact the primary contact or his/her supervisor. The emergency contact does not have to be a technical person.

If a system is housed or hosted outside of the CMS Baltimore Data Center facilities, an individual responsible for security and/or a component ISSO contact shall be provided for the contractor or external business partner hosting the system.

The assignment of security responsibility shall include the contacts following information:

- Name;
- Title;
- Organization;
- Address;
- Mail stop;
- City, State, Zip;
- E-mail;
- Telephone number: and
- Emergency Contact

SYSTEM OPERATIONAL STATUS

Instruction:
- Place a check (only one) in the applicable box that describes the system operational status.

Annotate whether the GSS, GSS sub-component, MA or MA individual application is either new, operational or undergoing a major modification.

DESCRIPTION OF THE BUSINESS PROCESS

Instruction:
Provide detailed descriptions regarding the various business processes.

Provide a brief description of the function and purpose of the system i.e. financial management, network support, business data analysis, research or procurement. The Business Owner and/or System Developer/Maintainer or author shall:

- Indicate the location of the system. This high-level description shall include the street address and other information pertaining to the location of the system;

- Describe the business function for each system;
- Describe the underlying business processes and resources that support each business function. This may include the required inputs (business functions/processes that feed this function), processing functions (calculations, etc), organizational/personnel roles and responsibilities, and expected outputs/products (that may “feed” other business functions / processes;
- Describe how information flows through/is processed by the system, beginning with system input through system output. Further describe how the data/information is handled by the system (is the data read, stored, purged, etc?);
- Indicate the organizations (internal & external) that will comprise the user community. Include type of data and processing that will be provided by users, if any; and
- Describe the users’ level of access to: system-related data (read-only, alter, etc), system-related facilities, and information technology resources.

If the system is a GSS, list all applications supported by the GSS and specify if the application is a MA and include unique name/identifiers, where applicable. Describe each application's function and the information processed.

DESCRIPTION OF OPERATIONAL / SYSTEM ENVIRONMENT AND SPECIAL CONSIDERATIONS

***Note: This section differs from the previous section in that it addresses the technical aspects of the system.**

Instruction:
Provide operational related information regarding:

- Communications requirements;
- User-interface expectations; and
- Network connectivity requirements.

Provide system related information regarding:

- System Environment;
- Architecture & Topology;
- Boundary Issues;
- Primary Platforms & Security Software;
- System Interconnectivity Interfaces, Web protocols, and computing environments; and
- Special Security concerns.

Attach the network connectivity diagram

Operational Information

Describe (at a high level) the anticipated technical environment and user community necessary to support the system and business functions. Include:

- Communications requirements;
- User-interface expectations; and
- Network connectivity requirements.

Be sure to indicate, the physical location of the business processes and technology that will support the system.

System Information

Provide a brief general description of the technical aspects of the system.
Include any environmental or technical factors that raise special security concerns, such as use of Personal Digital Assistants, wireless technology, etc.

Attach the network connectivity diagram, which shall address the system components' connection, and the security devices, which, 1) protect the system and, 2) monitor system access and system activity. For systems that have more than one server of the same type, only include one in the diagram, however state the accurate count of the servers in the supporting text description. Be sure to provide an opening sentence(s) prior to the diagram. Following the diagram, include text that will explain system components and function. Be sure to number system components in the diagrams to correlate with the information presented.

System Environment

Provide a description of the system environment:

- Is the system owned or leased?
- Is the system operated by the Government or by a support service contractor?
- If the system is maintained or "run" by a contractor, describe (comprehensively) how the system is managed.
- Document the hours of operation; e.g., 24x7, M-F 7:30 am – 5:00 pm.
- Document the approximate total number of user accounts and unique user types

(i.e., researchers, programmers, administrative support, etc.).

- Identify the critical processing periods (e.g., payroll processing.).
- If system serves a large number of off-site users, list both the organizations and types of users (e.g., other agencies.).
- List all applications supported by the system including the applications' functions and information processed.
- Describe how system users access the system (i.e., desktop, thin client, etc.). Include any information required to evaluate the security of the access.
- Describe the information / data stores within the system and security controls for such data.
- Describe how both the system's information and operation serve as an asset to CMS.
- Describe the purpose and capabilities of the information system.
- Describe the functional requirements of the information system. For instance:
  - Are protection mechanisms (i.e., firewalls) required?
  - Are support components such as web servers and e-mail required?
  - What types of access mechanisms (i.e., telecommuting, broadband communications) are required.
  - Are "plug-in" methods (Mobile code; Active-X, Javascript) required?
  - What operating system standards, if any, are required?

Architecture and Topology

Describe the architecture of the information system. If this is documented in another master or associated SSP, reference it by unique identifier and plan name.

- Describe the network connection rules for communicating with external information systems.
- Describe the functional areas within the architecture (presentation, application and data zones, if applicable) and how this addresses security.

Boundary Issues

Provide a detailed description of the system's boundaries and technical components.

- Describe the boundary of the information system for security accreditation.
- Describe the hardware, software, and system interfaces (internal and external) to include interconnectivity.
- Describe the network topology.
- Include a logical diagram for system components with system boundaries, if needed, to clarify understanding of the system function and integration.
- Following the logical diagram, describe the information flow or processes within the system to access to the data/information.

Primary Platforms and Security Software

Describe the primary computing platform(s) used and describe the principal system components, including hardware, firmware, software, wireless and communications resources. Include any environmental or technical factors that raise special security concerns (dial-up lines, open network, etc.). This will include vendors and versions.

- Include information concerning a system's hardware and platform(s).
- Detailed hardware equipment information, such as server names, shall be listed and attached to the documentation.
- Describe any security software protecting the system and information.
- Describe in general terms the type of security protection provided (e.g., access control to the computing platform and stored files at the operating system level or access to data records within an application). Include only controls that have been implemented, rather than listing the controls that are available in the software.

Interconnectivity Interfaces, Web Protocols and Distributed & Collaborative Computing Environments

Describe the Web protocols and distributed, collaborative computing environments (i.e., processes and applications).

- Describe the connectivity between modules within the scope of this system.
- For systems that interface with the Internet, describe how the architecture does/does not match the CMS Internet Platform Architecture.
- For any system that allows individual web-based access (Internet, Intranet, Extranet) to conduct transactions the following information should be provided:
  - The Uniform Resource Locator (URL) for the web-based transaction;
  - E-authentication architecture implemented;
  - E-authentication interoperable product used;
  - Other authentication products used;
  - Number of electronic log-ons per year;
  - Number of registered users (Government to Government);
  - Number of registered users (Government to Business);
  - Number of registered users (Government to Citizen);
  - Number of registered internal users; and
  - Description of customer groups being authenticated, e.g., Business Partners, Medicare Service Providers, Beneficiaries, etc.

Special Security Concerns

Include any environmental or technical factors that raise special security concerns, such as:

- Indicate the physical location of the information system;
- The system is connected to the Internet;
- It is located in a harsh or overseas environment;
- Software is implemented rapidly;
- The software resides on an open network used by the public or with overseas access; and
- The application is processed at a facility outside of CMS control.

SYSTEM INTERCONNECTION / INFORMATION SHARING

System interconnection is the direct connection of two or more IT systems for sharing information resources. It is important that Business Owners and management obtain as much information as possible regarding vulnerabilities associated with system interconnections and information sharing. This is essential in selecting the appropriate controls required to mitigate those vulnerabilities.

A CMS Interconnection Security Agreement (ISA) or CMS Memorandum of Understanding (MOU) is required between systems, which both share data, and are owned or operated by different organizations. If the system interconnection/information sharing is between two or more CMS system located internal to the CMS secure network infrastructure, the Business Owner shall utilize and follow the CMS MOU template. If the system interconnection / information sharing is between a CMS system and a system located external to the CMS secure network infrastructure, the Business Owner shall utilize and follow the CMS ISA template.

SYSTEM SECURITY LEVEL

Identify the system security level. Each system identified in the CMS system inventory must be categorized using CMS System Security Level by Information Type, which can be found at the CMS IS web-site, http://www.cms.hhs.gov/InformationSecurity/Downloads/ssl.pdf .

If multiple categories apply, the highest-level category is defined as the Sensitivity level for the system.

Instruction:

- Categorize the system based on the CMS System Security Level by Information Type in the table.
- Describe in general terms the information handled by the system and the protective measures.

E-AUTHENTICATION ASSURANCE LEVEL

Check the appropriate box concerning the system's /application's ability to provide web-based access to individuals for the purpose of conducting transactions. If web-based transactions are permitted, and RACF/Top Secret/Active Directory (or equivalent) is used to authenticate individuals, check the appropriate box.

Use the E-authentication Workbook to establish the level of security required for the system. The Workbook addresses all four (4) levels of assurance for E-authentication and has been developed into two aspects "Registration and Identify Proofing" and "Authentication Mechanism Requirements" that correspond to the four (4) system assurance levels.

APPLICABLE LAWS OR REGULATIONS

List any laws, regulations, specific standards, guidance or policies that establish specific requirements for CIA of data/information in the system. Possible laws, regulations, and judicial decrees for inclusion in the SSP shall include only those, which do not appear on the CMS IS website http://cms.hhs.gov/informationsecurity (Laws and Regulations)

Instruction:
Indicate laws, regulations and judicial decrees that may affect the system.

RULES OF BEHAVIOR (ROB)

Indicate the following information including but not limited to:

- A definition of each type of user of the system (e.g., user, developer, sys admin, DB admin) and a summary of the ROB or "code of conduct" specific to the 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;
- Password construction / maintenance;
- Changing system data;
- Searching databases;
- Divulging information;
- Working at home;
- Dial-in access;
- Connection to the Internet; and
- Assignment and limitation of system privileges.

Instruction:
Provide a definition for each type of user of the system, and a summary of the rules of behavior for each user type.

When developing the ROB for the specific SSP, reference the backside of the CMS form "Application for Access to CMS Computer Systems" that contains the enterprise-wide ROB and the Health and Human Services (HHS) requirements:

http://hhs.gov/ocio/policy/2008-0001.003s.html

Further, the ROB must include the consequences of non-compliance and must clearly state the exact behavior expected of each person. CMS shall address security controls and inherited risk from system users and the system administrator. If the system user is outside the system maintainer's purview, information shall be included from the Business Owner and/or System Developer/Maintainer's perspective.

REVIEW OF SECURITY CONTROLS

Provide information regarding any reviews that have been conducted in the past twelve (12) months. A review of security controls by the Business Owner at least once every three hundred and sixty five (365) days is required to be performed for all systems. In addition, other reviews, audits, assessments can be performed on the system and must be described in this section.

Instruction:

- Provide information regarding any reviews that have been conducted in the past twelve (12) months.
- Indicate the anticipated testing schedule for the system.

If a security evaluation was conducted within the past twelve (12) months, the following information must be provided:

- Who performed the review;
- When was the review was performed;
- What was the purpose of the review;
- A summary of general findings;
- A list of actions taken as a result of the review; and
- A reference to the location of the full report and corrective action plans.

Further, use this space to indicate the anticipated security control review schedule for the system.

RISK ASSESSMENT AND RISK MANAGEMENT

The RA must describe the methods used to assess the nature and level of risk to the system. State the RA methodology used and describe if it is different from the CMS IS RA Procedure. The results of the RA, using the CMS IS RA Procedure, must be documented and provided in the SSP. Any acceptance of these risks should also be indicated in the certification forms with the SSP. The CIO will take this information into consideration when reviewing the system for accreditation. Assessing the risk to a system is an on-going activity to ensure that new threats and vulnerabilities are identified and appropriate security measures are implemented. Further information on the CMS IS RA Procedure can be found at the CMS IS web-site:

Instruction:
Indicate the RA methodology used, and description as appropriate.

http://cms.hhs.gov/informationsecurity/downloads/RA_procedure.pdf

The use of an RA process other than the CMS IS RA Procedure is strongly discouraged and could delay the processing of the system for accreditation. If a non-CMS IS RA process is used and 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.

The table in section 1.13 of the SSP template should be completed for all of the system-specific vulnerabilities. The vulnerabilities included in the table should map directly to the RA report as follows:

- IS RA, Risks and Safeguards table, field titled ‘Vulnerability Name’ corresponds to SSP, Section 1.13 table, column titled ‘Vulnerability’;
- IS RA, Risks and Safeguards table, field titled ‘Risk Level’ corresponds to SSP, Section 1.13 table, column titled ‘Risk Level’;
- IS RA, Risks and Safeguards table, field titled ‘Recommended Safeguard Description' corresponds to SSP Section 1.13 table, column titled ‘Recommended Safeguard’;
- IS RA, Risks and Safeguards table, field ‘Residual Risk Level’ corresponds to SSP Section 1.13 table, column titled ‘Residual Risk’;
- Column titled ‘Status of Safeguard’ of the SSP - RA and Risk Management table in Section 1.13 describes the implementation status of recommended safeguard; and
- Column titled ‘Updated Risk’ of the SSP RA and Risk Management table in Section 1.13 describes risk level based on the implementation status of the recommended safeguard. If the recommended safeguard is not fully implemented and any implementation to date changes the risk level for the evaluated threat / vulnerability pair, the Updated Risk shall be changed accordingly.

PLANNING FOR SECURITY IN THE SDLC

Instruction:
Describe the implementation of security in each phase of the Framework.

Identify how security is implemented in the "Framework" phases. For instance:

- How was the System Sensitivity level ascertained? When? In what phase?
- How were the initial security requirements defined? When were they tested?

All legacy systems and systems developed by CMS through the Investment Planning Management Process (IPMP) need only refer to the CMS Master Plan (CMS Master Plan addresses Administrative and Physical security).

SECURITY CONTROLS DETAIL AND COMMENT

Instruction:

- Describe the strategy used in implementing the security controls of each control family.
- Document the baseline configuration of the system. Include appendices showing the baseline configuration
- Document the component or contractor responsible for the control

- Describe how the security controls are implemented for each of the eighteen (18) control families using the information documented within the SSP Workbook. Section 1 and Section 2.1 within the Workbook, provide the steps to populate the information from the workbook into the SSP.
- Discuss in detail, the strategy used in implementing the controls.
- Include in the Configuration Management (CM) control section the baseline security configurations of the system/application. The *CMS Minimum Security Configuration Standards.* (see https://www.cms.hhs.gov/cbt/downloads/IS_baseline_configs.pdf) was created to supply standards for configuring CMS systems and applications using minimum standards for the products currently defined. Other configuration guidance can be found in NIST Special Publications-800 series and the Defense Information Systems Agency (DISA) configuration guides. More information on configuration management can be found in the *Business Partners System Security Manual (BPSSM).* (see http://www.cms.hhs.gov/transmittals/downloads/R9SS.pdf) To resolve configuration conflicts among multiple security guidelines, the CMS hierarchy for implementing all security configuration guidelines is as follows CMS, DHHS, OMB, NIST, then DISA. Except for the CMS standard baselines, CMS does not require the verbatim use of these guidance documents and tools but does require that an active configuration management program be established and maintained for the system / application. Since the specific baseline security configurations supporting the systems can be voluminous, in this section a cross-reference to Appendix C Detailed Configuration Settings is acceptable. For this appendix alone, an electronic attachment can be provided containing the detailed configuration settings that satisfy the required CMS baseline configurations. Please note that any exceptions to the standard CMS baselines accepted by CMS must be documented as part of the SSP.
- An HHS waiver form must be completed for each alternative setting to the CMS baselines. As an alternative to using the waiver form, since most of the CMS standard baselines are in tabular format, you may chose to provide the information solicited in the waiver form in additional columns for each particular setting for which your system or application utilizes a standard other than the one stipulated in the baseline. Remember to include all the information solicited on the waiver form if you choose the alternate method. Requests for waivers must submitted through the CMS CISO.
- .At the bottom of each control section, document the organizational component or contractor responsible for supporting and maintaining the control. If contractor information is supplied, indicate the CMS component that manages that contract,

i.e., the component (Division Level or above) of the Government Task Lead or the Project Officer.

- When applicable, it is acceptable for the author to cut and paste the "Security Controls Detail and Comment" information from the workbook into the SSP template. However, the details and comments contained within the SSP template will be considered the information of record. Therefore, great care must be taken to ensure that the SSP template contains accurate and up to date information.
- Document any changes to the controls since the last review.

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. At a minimum, the SSP must contain the following Appendices:

- Appendix A - This appendix contains a listing of equipment that supports the System/Application. This appendix should be labeled as APPENDIX A – EQUIPMENT LIST;
- Appendix B - This appendix contains a listing of software that support the System/Application. This appendix should be labeled as APPENDIX B – SOFTWARE LIST;
- Appendix C – This appendix contains the detailed configuration settings that satisfy the required CMS baseline configurations. This appendix should be labeled as APPENDIX – C DETAILED CONFIGURATION SETTINGS;
- Appendix D – This appendix contains the glossary of terms used in the SSP and is provided for additional clarity. For Glossary of Terms and Acronyms refer to http://cms.hhs.gov/informationsecurity/. Add only the terms that are referenced in the SSP and not found on the website. This appendix should be labeled as APPENDIX – D GLOSSARY; and
- Appendix E – This appendix contains the acronyms and abbreviations used in the SSP and are provided for additional clarity. This appendix should be labeled as APPENDIX – E ACRONYMS AND ABBREVIATIONS.

Attachments are used to provide supplemental detailed information. If needed supplemental detailed information can be provided as an attachment to the SSP. The attachment should be labeled as ATTACHMENT and listed in alphabetical sequence with the subject title of the attachment.

APPENDIX B: ACRONYMS

AFS	Administrative Finance System
ARS	Acceptable Risk Safeguard
BPSSM	Business Partners Systems Security Manual
BUCS	Budget Under Control System
C&A	Certification & Accreditation
CAP	Corrective Action Plan
CHRIS	CMS Human Resources Information System (CHRIS)
CIA	Confidentiality, Integrity, Availability
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CMS	Centers for Medicare & Medicaid Services
CMSR	CMS Minimum Security Requirements
DISA	Defense Information Systems Agency
DITPPA	Division of Information Technology, Policy, Procedures, & Audits
EASG	Enterprise Architecture & Strategy Group
EUA	End User Agreement
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act of 2002
FMIB	Financial Management Investment Board
FRAMEWORK	CMS IT Investment Integrated System Development Life-cycle
GAO	General Accountability Office
GSS	General Support System
HRMS	Human Resource Management System
IS	Information Security
ISA	Interconnection Security Agreement
ISSO/SSO	Information System Security Officer/System Security Officer
IS RA	Information Security Risk Assessment
IT	Information Technology
ITIRB	Information Technology Investment Review Board
MA	Major Application
MOU	Memorandum of Understanding
NARA	National Archives and Records Administration
NIST	National Institute of Standards and Technology
OIG	Office of the Inspector General
OIS	Office of Information Services
OMB	Office of Management and Budget
PC	Personal Computer
PISP	CMS Policy for the Information Security Program
POA&M	Plan of Action & Milestone
RA	Risk Assessment
RAD	Rapid Application Development
RACF	Resource Access Control Facility

RM	Risk Management
SCT	Security Control Testing
SDLC	System Development Life-cycle
SP	Special Publications
SOR	System of Records
SSP	System Security Plan
ST&E	Security Test & Evaluation
URL	Uniform Resource Locator
WAN	Wide Area Network

ATTACHMENT 1: SSP PACKAGING INSTRUCTIONS

SSP DOCUMENTATION

To create a usable and functional SSP, the Business Owner or System Developer / Maintainer must keep the SSP package in a three (3) 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, specific risks in the IS RA). 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.

PACKAGING THE SSP

The SSP forms part of Tab C – System Security Plan (SSP)/Information Security (IS) Risk Assessment (RA) of the C&A package. The documentation required for the packaging of the SSP consists of the following:

- SSP;
- IS RA;
- Applicable Appendices;
- Applicable Attachments;
- Applicable Summaries;
- Applicable Reviews; and
- References Utilized.

The details for packaging the C&A Package items can be found in the CMS Information Security (IS) Certification & Accreditation (C&A) Program Procedure located at:

http://www.cms.hhs.gov/informationsecurity/downloads/CA_procedure.pdf

NOTE: The completed SSP 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. Our goal is to reduce to the minimum the effort needed by developers to produce functioning, workable systems.

End of Document