System Security Plan (SSP) and/or Information Security (IS) Risk Assessment (RA)

Summary Description:

As required by the Federal Information Security Management Act (FISMA) of 2002, all CMS information systems that store or process sensitive information must be covered by a System Security Plan (SSP). The SSP contains descriptions of the actual managerial, technical and operational controls, documenting the current level of security implemented within the system.

CMS has established a hierarchical structure for the development of SSPs. At the highest level is the CMS Master Security Plan, which defines the enterprise-level security controls that are in place within CMS. The Master Security Plan documents all of the security attributes that are standard enterprise-wide (e.g., personnel controls, overarching physical controls for the CMS site, contingency planning and disaster recovery, etc.). All lower-level SSPs inherit the attributes of the Master Security Plan, unless otherwise documented in that lower-level SSP.

Subordinate to the Master Security Plan are SSPs for each General Support System (GSS), which document all the security attributes of a specific GSS (e.g., review of security controls, physical and environmental protection specific to the GSS, production input/output, etc.). A GSS is a grouping of systems that consist of interconnected information resources under the same direct management control that share common functionality. A GSS normally includes hardware, software, information, data, applications, communications, facilities, and provides general support for a variety of users and/or applications. As a rule of thumb, a GSS is a physical platform and infrastructure upon which applications run (e.g., mainframe systems, web servers, communications equipment, etc.). All CMS internal system infrastructure is accountable within one of six GSS SSPs (i.e., CMS Data Center, Regional Offices, Web Hosting, Medicare Data Communications Network (MDCN), QualityNet, and Medicare Data Centers).

Subordinate to the GSS SSPs are SSPs for each of 15 established Major Applications (MA). A MA is a grouping of CMS application systems that support clearly defined business functions for which there are readily identifiable security considerations and needs (e.g., Administrative Finance Systems, Customer Service Systems, Managed Care Systems, Medicare Beneficiary Enrollment Systems, etc.). A MA is usually comprised of multiple application systems and occasionally might have hardware, software, and telecommunication components. These components can be a single software application or a combination of hardware/software focused on supporting a specific business-related function. MA SSPs only need to document the security controls specific to the MA and how, if applicable, their system adds to or deviates from the controls supported by the higher-level GSS and/or Master Plan.

In addition to the SSP, an Information Security (IS) Risk Assessment (RA) must be

conducted for each GSS, GSS sub-system (if applicable), MA and MA application. The IS RA contains a list of system threats and vulnerabilities, an evaluation of current system security controls, their resulting risk levels, and any recommended safeguards to reduce the system's risk exposure. Also, the IS RA supports risk management in the evaluation of the system's risk impact upon CMS' enterprise security model.

The SSP and the corresponding IS RA are key components of the CMS IS Certification and Accreditation (C&A) process and are the instruments used by the CMS Chief Information Officer (CIO) to evaluate and determine whether or not to grant authorization to process (i.e., System Accreditation or System Re-Accreditation. Similarly, the SSP and IS RA form the primary reference documentation for security testing and evaluation, whether by CMS, the General Accounting Office (GAO), the Office of the Inspector General (OIG), or other oversight bodies.

Status:

Mandatory - The requirement for a System Security Plan (SSP) and an Information Security (IS) Risk Assessment (RA) applies to all CMS information systems and installations, whether developed and/or maintained in-house or hosted off-site, and to all External Business Partner information systems and installations operated by or for CMS (e.g., External Business Partner sites). Additionally, the controls documented in the SSP and IS RA must apply to all employees and personnel from other organizations, including contractor personnel, sub-contractors and vendors using or participating in the development, operation and maintenance of the CMS information system and installation. Full management approval to operate a CMS information system (accreditation) is granted by the CIO for a period of three years following which the SSP and IS RA must be updated and resubmitted for Certification & Accreditation (C&A). Interim accreditations (conditional approval to operate) can be for no longer than one year. However, if there is a major system modification(s), increased security risks/exposure, increase of overall system security level, a serious security violations(s), or a critical finding as a result of security evaluations and/or audits, the SSP and IS RA must be updated and resubmitted for C&A. If an information system is not covered by an existing SSP, the System Owner/Manager is required to determine the appropriate CMS GSS or MA for the information system. For a description of each of the existing GSSs and MAs, see CMS GSSs and MAs (PDF - 44KB). The SSP and IS RA are reviewed during System Certification, System Accreditation, System Re-Certification, and System Re-Accreditation.

Timeframe:

The System Security Plan (SSP) and/or Information Security (IS) Risk Assessment (RA) are initiated during the Requirements Analysis Phase and are initially baselined during the Design & Engineering Phase. The SSP and/or IS RA continue to be enhanced throughout the Development Phase and must be completed prior to System Certification, System Accreditation, and the Operational Readiness Review that are respectively performed during the Implementation & Testing Phase. During the Operations &

Maintenance Phase, the SSP and/or IS RA are updated prior to System Re-Certification and System Re-Accreditation every three years or when there is a major system modification(s), increased security risks/exposure, increase of overall system security level, a serious security violation(s), or a critical finding(s) as a result of security evaluations and/or audits.

Responsible Reviewing Component:

OIS/SSG is the CMS component that has the primary decision authority over the need for a System Security Plan (SSP) and/or an Information Security (IS) Risk Assessment (RA), requirements for its creation, and acceptance of the end product in meeting the information needs.

Primary Information Exchange Partners:

The following are the primary stakeholders who have an interest in the content of the System Security Plan (SSP) and/or Information Security (IS) Risk Assessment (RA):

Project Owner/Manager
System Owner/Manager
System Developer
System Maintainer
IV&V Contractor
Certification & Accreditation (C&A) Evaluator
Component Information Systems Security Officer (ISSO)
Senior Information Systems Security Officer (ISSO)
Chief Information Officer (CIO)
Chief Technology Officer (CTO)
General Accounting Office (GAO)
Office of the Inspector General (OIG)

Government Responsibilities:

The Project Owner/Manager and System Owner/Manager are responsible for meeting with OIS/SSG to determine if the information system is included within an existing General Support System (GSS) or Major Application (MA) System Security Plan (SSP), and to discuss the requirements for the SSP and/or Information Security (IS) Risk Assessment (RA) based on the circumstances of the specific IT project.

The System Owner/Manager and System Developer are responsible for preparing an SSP, if necessary, that provides a description of the security and privacy requirements of the information system and the plan for meeting those requirements. The System Owner/Manager and System Developer are responsible for conducting risk assessments, implementing controls determined to be required and cost-effective, and developing contingency and disaster recovery plans that ensure availability of the system for mission accomplishment.

To perform the IS RA, the System Owner/Manager and System Developer must identify the system's threats and associated vulnerabilities. For each threat/vulnerability pair, the System Owner/Manager and System Developer determine the severity of impact upon the system's confidentiality, integrity, and availability, and determine the likelihood of the vulnerability exploit occurring given existing security controls. The product of the likelihood of occurrence and the impact severity results in the risk level for the system based on the exposure to the threat/vulnerability pair. Safeguards are then identified for threat/vulnerability pairs with moderate or high-risk levels. The risk is re-evaluated to determine the remaining risk, or residual risk level, after the recommended safeguard is implemented.

The System Owner/Manager is responsible for keeping the SSP and/or IS RA for the information system in a three-ring binder to maintain a history of all documentation and sign-offs related to the security planning process. The SSP and/or IS RA are to be used by all CMS individuals with defined responsibilities for information security at the system and organizational level, which includes the System Maintainer, Component Information Systems Security Officer (ISSO), Senior Information Systems Security Officer (ISSO), Chief Information Officer (CIO), and Chief Technology Officer (CTO).

Contractor Responsibilities:

The following are responsibilities that the System Developer has with regard to the System Security Plan (SSP) and/or Information Security (IS) Risk Assessment (RA). If a contractor is tasked with developing the information system, then these are the responsibilities of the development contractor. If the information system is being developed by in-house CMS staff, then these are the responsibilities of the government developers.

The System Developer shall engage in the following activities, which will form the basis for completing the SSP and/or IS RA:

1. Security Assurance: Identify as security-critical those computer software configuration items or portions whose failure could lead to a breach of system security. If there is such software, the System Developer shall develop, document and implement a security assurance strategy to assure that the requirements, design, implementation, and operating procedures for the identified software minimize or eliminate the potential for breaches of system security. The System Developer shall produce evidence that the security assurance strategy has been put into practice.

2. Privacy Assurance: Identify as privacy-critical those computer software configuration items or portions whose failure could lead to a breach of system privacy. If there is such software, the System Developer shall develop, document and implement a privacy assurance strategy to assure that the requirements, design, implementation, and operating procedures for the identified software minimize or eliminate the potential for breaches of

system privacy. The System Developer shall produce evidence that the privacy assurance strategy has been put into practice.

Content:

The System Security Plan (SSP) documents controls that are implemented and tested to provide protection from threats and vulnerabilities identified during the planning and review process. At a minimum, the SSP must include: identifying information about the system; overall management controls currently implemented; day-to-day procedures and mechanisms serving as operational controls; technical controls; and any additional relevant supporting documentation. For more information regarding the content and format of the SSP, see the System Security Plan (SSP) Methodology. The SSP Template is contained in the SSP Methodology or is available separately in the System Security Plan (SSP) Template.

The Information Security (IS) Risk Assessment (RA) includes a system overview to provide a basic understanding of the system and its interconnections, and describes the overall system security level. Additionally, the IS RA contains a list of system threats and vulnerabilities; an evaluation of current security controls to safeguard against the identified threat/vulnerability pairs and the resulting risk levels; and the recommended safeguards to reduce the system's risk exposure with a revised or residual risk level once the recommended safeguards are implemented. For more information regarding the content and format of the Information Security RA, see the CMS Information Security (IS) Risk Assessment (RA) Methodology. The RA Template is contained in the IS RA Methodology or is available separately in the CMS Information Security (IS) Risk Assessment (RA) Template.

Guidance:

For guidance in the development of a System Security Plan (SSP), see the System Security Plan (SSP) Methodology. This methodology provides a specific format for the SSP, and should be followed to ensure that the developed SSP complies with CMS information security standards. The SSP Template is contained in the SSP Methodology or is available separately in the System Security Plan (SSP) Template.

For guidance in the development of an Information Security (IS) Risk Assessment (RA) see the CMS Information Security (IS) Risk Assessment (RA) Methodology. The RA methodology provides a systematic and qualitative approach for conducting a CMS IS RA and the steps to follow to produce the required report. The IS RA Template is contained in the IS RA Methodology or is available separately in the CMS Information Security (IS) Risk Assessment (RA) Template.

For additional guidance on how an IS RA and SSP shall be structured and developed, contact OIS/SSG.

Review Process:

The System Owner/Manager, the System Maintainer, and the Component Information Systems Security Officer (ISSO) review and formally approve the SSP and/or IS RA during System Certification. An IV&V Contractor may also be utilized to review the SSP and/or IS RA. After completion of System Certification, the SSP and/or IS RA are reviewed and tested by an independent Certification & Accreditation (C&A) Evaluator assigned by OIS/SSG. Based on the evaluations and recommendations of the C&A Evaluator and the Chief Technology Officer (CTO), the Chief Information Officer (CIO) grants the authorization to process during System Accreditation. Subsequent updates to the SSP and/or IS RA are reviewed and formally approved during System Re-Certification and System Re-Accreditation.

Date Created/Modified:

March 2002/February 2005