

# What Is A Deliverable?

Deliverables are documentation artifacts that are to be produced during the CMS IT Investment Management Process.

There are two main categories of deliverables: Investment Management Level and Project Management Level.

**Investment Management Level Deliverables** are documentation artifacts that are to be produced during the system life cycle which are mandatory or conditionally mandatory for all IT projects (with limited exceptions) and are input to an Investment Management Level Review(s).

**Project Management Level Deliverables** are documentation artifacts that are to be produced during the system life cycle which are input to a Project Management Level Review(s).

The following is a list of the CMS **Investment Management Level Deliverables**, presented as links to more detailed information regarding the identified deliverables. The information available in the Roadmap for each deliverable consists of a Summary Description and Status for the deliverable, as well as the identified Lifecycle Phase(s) during which the deliverable is initiated and/or completed. In addition, Guidance is provided for the generation of each deliverable, such as identified points of contact, documentation references, templates, samples or development guides that can assist in the development of the deliverable.

[IT Fact Sheet](#)

[HHS-393 Form](#)

[Business Case Analysis \(BCA\) Statement of Work \(SOW\) / HHS-393 Form](#)

[Business Case Analysis \(BCA\)](#)

[Exhibit 300](#)

[System Development Life Cycle \(SDLC\) Statement of Work \(SOW\) / HHS-393 Form](#)

[Contractor Proposal](#)

[ITA Conformance Certification Checklist](#)

[Data Use Agreement \(DUA\)](#)

[System of Records \(SOR\)](#)

[Computer Match Agreement \(CMA\)](#)

[Inter/Intra-agency Agreement \(IA\)](#)

[Implementation Readiness Review \(IRR\) Data Sheet](#)

[System Security Plan \(SSP\)](#)

[System Security Plan \(SSP\) Certification Form](#)

[System Security Plan \(SSP\) Accreditation Form](#)

The CMS **Project Management Level Deliverables** are still in the process of being identified.

# IT Fact Sheet

## Summary Description:

The IT Fact Sheet is a form in the IT Investment Tracking Database that a Project Owner / Manager must complete to obtain funding for any IT project. The IT Fact Sheet contains basic information about the project (e.g., project description, prevailing business need, projected cost for the current fiscal year and the out years, anticipated benefits, major milestones and timeline, potential technical strategies, performance measures, potential risk, and a spending plan). The Project Owner/Manager maintains the IT Fact Sheet throughout the year to make sure that the information is current. The cost sections are updated annually to provide information to the Financial Management Investment Board (FMIB) when preparing the Operating Plan for the next fiscal year. In addition, the Project Owner/Manager must complete two questionnaires linked to the IT Fact Sheet. The first is a Technical Evaluation that contains preset questions about the hardware, software, and platform components of the project. The second is a set of eight questions established in OMB Circular A-130 (formally known as “Raines Rules”) that address the need and implementation strategy of the project, which must be answered for all new major information systems projects (Levels C and D).

## Status:

**Mandatory - Investment Management Level Deliverable** - All IT projects (Levels A, B, C and D) must have a complete IT Fact Sheet maintained in the IT Investment Tracking Database.

## Lifecycle Phase:

The IT Fact Sheet is initially completed during the Investment Analysis Phase, but is continually maintained by the Project Owner/Manager throughout the remaining phases of the system life cycle.

## Guidance:

For information regarding the content of the IT Fact Sheet, see [IT Fact Sheet Content](#).

For guidance in the completion of the IT Fact Sheet and/or to obtain access authorization to the IT Investment Tracking Database, contact [OIS/PMSG/DIAB](#).

# HHS-393 Form

## Summary Description:

The HHS-393 Form is the official CMS funding requisition document that must be prepared and approved for the procurement of goods and/or services.

## Status:

**Mandatory - Investment Management Level Deliverable** - All IT projects (Levels A, B, C and D) must prepare a HHS-393 Form in order to purchase information technology goods and/or services.

## Lifecycle Phase:

A HHS-393 can be prepared at any time during the system life cycle, as necessary and appropriate. However, a HHS-393 must be prepared during the Investment Analysis Phase in conjunction with a Statement of Work (SOW) for all new IT projects that will utilize a contractor to develop a Business Case Analysis (BCA). In addition, a HHS-393 must be prepared during the Acquisition Phase in conjunction with a Statement of Work (SOW) for all IT projects that will utilize a contractor to perform work during the System Development Life Cycle (SDLC).

## Guidance:

For an electronic copy of the HHS-393 Form, see:

[HHS-393 Form Template \(Word Version\)](#)

[HHS-393 Form Template \(PDF Version\)](#)

For written instructions on preparing the HHS-393 Form, see [HHS-393 Form Instructions](#).

For guidance in the completion of the HHS-393 Form, contact [OIS/PMSG/DIAB](#).

# **Business Case Analysis (BCA) Statement of Work (SOW) / HHS-393 Form**

## **Summary Description:**

After funding for the Business Case Analysis (BCA) has been approved by the Financial Investment Management Board (FMIB), a Statement of Work (SOW) is prepared that provides a complete description of the work to be performed by a contractor in the development of a BCA. The SOW encompasses all specifications and standards established or referenced in the contract. The SOW must clearly state the obligations and responsibilities of both the contractor and the government. The SOW must also provide clear, complete directions so that the contractor using the SOW alone (without interpretation by the Government Task Leader (GTL)) can prepare a BCA for the project in an effective and efficient manner. In conjunction with a SOW for the BCA contract, a corresponding HHS-393 Form, which is CMS' official funding requisition document for procuring goods and/or services, must also be prepared and approved.

## **Status:**

**Conditionally Mandatory - Investment Management Level Deliverable** - All new IT projects (Levels B, C and D) that will utilize a contractor to develop a Business Case Analysis (BCA) must prepare a Statement of Work (SOW) / HHS-393 Form. The CIO Planning, Management, and Support Group (PMSG) of the Office of Information Services (OIS) has awarded a task-order contract to provide ongoing assistance to Project Owners/Managers in developing the BCA. PMSG strongly encourages the use of this contractor since it will provide expertise and objectivity in preparing the BCA. This BCA contractor, however, is ineligible to perform the actual systems development support work for the project in the later IT Investment Management Phase.

## **Lifecycle Phase:**

The Business Case Analysis (BCA) Statement of Work (SOW) / HHS-393 Form is initiated and completed during the Investment Analysis Phase. The completed BCA SOW/HHS-393 Form serves as input to the Review of BCA SOW/393 also performed during the Investment Analysis Phase.

## **Guidance:**

For information regarding the format and content of a sample BCA SOW, see:  
[BCA SOW Sample \(Word Version\)](#)  
[BCA SOW Sample \(PDF Version\)](#)

For additional guidance in the development of the BCA SOW, contact [OIS/PMSG/DIAB](#).

For detailed information regarding the HHS-393 Form, see [HHS-393 Form](#).

# Business Case Analysis (BCA)

## Summary Description:

The Business Case Analysis (BCA) establishes sound business reasons for proceeding with a project by providing insight into how the project supports business needs and the strategic goals of CMS. The BCA describes how the project aligns with CMS's Information Technology Architecture (ITA) and identifies the project's assumptions and constraints. The BCA identifies the gap between current capability and new business needs, discusses alternatives for accomplishing the project, contains a cost/benefit analysis that is consistent with the preferred alternative, and presents a high-level logical design. The design verifies that the proposed solution will be compatible with the CMS architecture and begins to establish the impact of the project on the infrastructure. The BCA next provides an assessment of business risks, describes the acquisition strategy, and outlines the project plan. Finally, an appendix containing the documented and validated user and system requirements shall be included. Additional details of the alternatives analysis may also be included as an appendix, if necessary. The BCA allows the Financial Management Investment Board (FMIB) to make an informed decision about funding the project based on the scope, the cost, and the short and long-term impact.

## Status:

**Mandatory - Investment Management Level Deliverable** - All new IT projects (Levels B, C and D) must complete a Business Case Analysis to support the Financial Management Investment Board (FMIB) investment funding decision.

## Lifecycle Phase:

The Business Case Analysis (BCA) is initiated and completed during the Investment Analysis Phase. The completed BCA serves as input to the Review of Business Case Analysis (BCA) also performed during the Investment Analysis Phase.

## Guidance:

For information regarding the content of the BCA, see Business Case Analysis Development Guide.

For additional guidance in the development of a BCA, contact OIS/PMSG/DIAB.

## Exhibit 300

### Summary Description:

The Exhibit 300 is an annual document required by the Office of Management & Budget (OMB) as part of the Clinger-Cohen Act for all Level D IT projects that have been listed individually in the President's Budget Submission. The Exhibit 300 contains three major sections: 1) a summary of spending for all of the project phases; 2) justification and other information; and 3) original baseline and current cost, schedule, and performance goals. An initial Exhibit 300 is prepared based on the results of the Business Case Analysis (BCA). In subsequent years, there is a focus on the third section of the Exhibit 300 comparing the baseline information with the current project status.

### Status:

**Conditionally Mandatory - Investment Management Level Deliverable** - All Level D IT projects that have been listed individually in the President's Budget Submission must have an Exhibit 300 prepared upon completion of the Business Case Analysis (BCA) and subsequent investment approval from the Financial Management Investment Board (FMIB). In addition, an updated Exhibit 300 must also be prepared on an annual basis throughout the remainder of the system development life cycle. The Division of Investment Analysis and Budget (DIAB) in the CIO Planning, Management, and Support Group (PMSG) of the Office of Information Services (OIS) is responsible for preparing the Exhibit 300 based on information provided by the Project Owner/Manager. The Project Owner/Manager is not responsible for preparing the Exhibit 300, but is responsible for providing OIS/PMSG/DIAB with requested information necessary for the completion of this deliverable.

### Lifecycle Phase:

The Exhibit 300 is initially completed during the Acquisition Phase, but is updated on an annual basis thereafter regardless of the lifecycle phase that the project is currently in at the time. The completed initial Exhibit 300 serves as input to the Initial Department/OMB Clearance also performed during the Acquisition Phase, while the completed annual Exhibit 300 serves as input to the Annual Department/OMB Clearance review process.

### Guidance:

For additional information regarding the completion of the Exhibit 300, contact OIS/PMSG/DIAB.

# **System Development Life Cycle (SDLC) Statement of Work (SOW) / HHS-393 Form**

## **Summary Description:**

After the Business Case Analysis (BCA) is accepted and the project receives funding approval to proceed, a Statement of Work (SOW) is prepared to obtain the services of a contractor to begin activities in one or more phases of the system development life cycle (SDLC). A project may require multiple contractors to complete the work, therefore, there may be multiple SOWs needed. The SOW(s) prepared must provide a complete description of the work to be performed by the contractor(s). The SOW encompasses all specifications and standards established or referenced in the contract. The SOW must clearly state the obligations and responsibilities of both the contractor and the government. The SOW must also provide clear, complete directions so that the contractor using the SOW alone (without interpretation by the Government Task Leader (GTL)) can perform the work in an effective and efficient manner. In conjunction with the SOW(s), a corresponding HHS-393 Form(s), which is CMS' official funding requisition document for procuring goods and/or services, must also be prepared and approved.

## **Status:**

**Conditionally Mandatory - Investment Management Level Deliverable** - All IT projects (Levels B, C and D) that will utilize a contractor to perform work during the System Development Life Cycle (SDLC) must prepare a Statement of Work (SOW) / HHS-393 Form.

## **Lifecycle Phase:**

The System Development Life Cycle (SDLC) Statement of Work (SOW) / HHS-393 Form is initiated and completed during the Acquisition Phase. The completed SDLC SOW / HHS-393 Form serves as input to the Review of SDLC SOW/393 also performed during the Acquisition Phase.

## **Guidance:**

For an electronic copy of a template for preparing a SDLC SOW, see:

[SDLC SOW Template \(Word Version\)](#)

[SDLC SOW Template \(PDF Version\)](#)

For additional guidance in the development of the SDLC SOW, contact [OIS/PMSG/DIS](#).

For detailed information regarding the HHS-393 Form, see [HHS-393 Form](#).

# Contractor Proposal

## Summary Description:

A Contractor Proposal is an offer submitted by a contractor in response to a Request for Proposal (RFP) or Statement of Work (SOW) issued by CMS during the system development life cycle (SDLC).

## Status:

**Conditionally Mandatory - Investment Management Level Deliverable** - A Contractor Proposal is a deliverable that CMS receives from one or more contractors in response to the System Development Life Cycle (SDLC) Statement of Work (SOW) released by CMS to prospective offerors via a Request for Proposal (RFP) action.

## Lifecycle Phase:

A Contractor Proposal is a deliverable that is received during the Acquisition Phase from one or more contractors in response to the System Development Life Cycle (SDLC) Statement of Work (SOW). The Contractor Proposal(s) serve as the input to the Proposal Review & Award process also performed during the Acquisition Phase.

## Guidance:

For information regarding the request for, receipt and evaluation of Contractor Proposals, contact OICS/AGG.

# ITA Conformance Certification Checklist

## Summary Description:

The Information Technology Architecture (ITA) Conformance Certification Checklist is a document that is to be completed by the Project Owner/Manager for the purpose of self-assessing that an IT system is in conformance with CMS's ITA standards. The completed ITA Conformance Certification Checklist is utilized as an input to the CIO Initial IT Architecture Review and Certification performed during the Design & Engineering Phase for all Level C and D IT projects. The ITA Conformance Certification Checklist, updated as necessary, is also utilized as an input to the CIO Final IT Architecture Review and Certification performed during the Development Phase for all Level C and D IT projects.

## Status:

**Mandatory - Investment Management Level Deliverable** - All IT projects (Levels C and D) must have a completed ITA Conformance Certification Checklist. IT system development projects must satisfy the "Mandatory" criteria in order to be in conformance with the ITA. "Preferred" criteria are optional, but strongly encouraged.

## Lifecycle Phase:

The ITA Conformance Certification Checklist is initially completed during the Design & Engineering Phase, and is updated, if necessary, during the Development Phase. The completed ITA Conformance Certification Checklist serves as input to the CIO Initial IT Architecture Review and Certification also performed during the Design & Engineering Phase, as well as for the CIO Final IT Architecture Review and Certification process performed during the Development Phase.

## Guidance:

For an explanation of the ITA Conformance Criteria and guidance in completing the ITA Conformance Certification Checklist, see:

[ITA Conformance Certification Criteria Guide \(PDF\)](#)

For an electronic copy of the ITA Conformance Certification Checklist form, see:

[ITA Conformance Certification Checklist Template \(Word Version\)](#)

[ITA Conformance Certification Checklist Template \(PDF Version\)](#)

For a sample of a completed ITA Conformance Certification Checklist, see:

[ITA Conformance Certification Checklist Sample \(PDF\)](#)

For guidance in the completion of the ITA Conformance Certification Checklist, contact [OIS/PMSG/DASP](#).

# Data Use Agreement (DUA)

## Summary Description:

A Data Use Agreement (DUA) is a legal binding agreement between CMS and an external entity (such as a CMS contractor, private industry, academic institution, other Federal government agency, or state agency), when an external entity requests the use of CMS personal identifiable data that is covered by the Privacy Act of 1974. The agreement delineates the confidentiality requirements of the Privacy Act, security safeguards, and CMS's data use policies and procedures. The DUA serves as both a means of informing data users of these requirements and a means of obtaining their agreement to abide by these requirements. Additionally, the DUA serves as a control mechanism through which CMS can track the location of its data and the reason for the release of the data. A DUA requires that a System of Records (SOR) be in effect, which allows for the disclosure of the data being used. The Office of Information Services (OIS) / Enterprise Databases Group (EDG) / Division of Data Liaison and Distribution (DDLDD) is responsible for establishing CMS guidelines and policies for the language in the DUA and coordinates the requests for use of personal identifiable data.

## Status:

**Conditionally Mandatory - Investment Management Level Deliverable** - All IT projects (Levels B, C and D) must prepare a Data Use Agreement (DUA) when a contractor(s) will be utilized to develop a system and will be required to access personal identifiable information for the purposes of developing the system. A DUA must also be prepared when an external entity (such as a CMS contractor, private industry, academic institution, other Federal government agency, or state agency) requests the use of CMS personal identifiable data from a system after it has been fully developed and is operating in the production environment. A DUA also requires that a System of Records (SOR) be in effect, which allows for the disclosure of the data being used.

## Lifecycle Phase:

A Data Use Agreement (DUA) must be initiated and completed during the Acquisition Phase when a contractor(s) will be utilized to develop a system and will require access to personal identifiable information covered by the Privacy Act of 1974 for the purposes of developing the system. The completed DUA developed during the Acquisition Phase serves as input to the Review of Data Use Agreement (DUA) also performed during the Acquisition Phase. A DUA must also be initiated and completed when an external entity (such as a CMS contractor, private industry, academic institution, other Federal government agency, or state agency) requests the use of CMS personal identifiable data from the system after it has become fully operational in the production environment. Thus, a DUA may also be required during the Operations & Maintenance Phase.

## Guidance:

For an electronic copy of the instructions and template for preparing a Data Use Agreement (DUA), see [Data Use Agreement \(DUA\) Template \(PDF\)](#).

For information regarding the preparation of a Data Use Agreement (DUA), contact [OIS/EDG/DDLD](#).

# System of Records (SOR)

## Summary Description:

The Privacy Act defines a System of Records (SOR) as a group of any records under the control of a Federal agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. Additionally, the Privacy Act requires that the Federal government inform the public of any collection of information about its citizens from which data are retrieved by a unique identifier as described above. CMS fulfills this requirement to inform the public via the publication of a system notice in the *Federal Register*. This notice describes the SOR and gives the public an opportunity to comment. Without the written consent of the subject individual, the Privacy Act prohibits the release of protected information maintained in a SOR unless one of the 12 disclosure exceptions apply. Therefore, a SOR is completed by the System Owner/Manager and consists of three documents: a Narrative Statement that is submitted to the Office of Management & Budget (OMB), and a Preamble and Statement of Records Notice that are provided to Congress. The Preamble and the Statement of Records Notice are also published in the *Federal Register* to notify the public of a new or revised SOR.

## Status:

**Mandatory - Investment Management Level Deliverable** - All IT projects (Levels B, C and D) that will cause CMS or its agents to collect, maintain, use or disclose information about a citizen of the United States (beneficiaries or individual health care providers), or transmit or maintain electronically any identifiable health information, must have a System of Records (SOR). For new systems that do not have an existing SOR, the Privacy Act Staff in OIS/EDG/DDLD must be notified six (6) months in advance of any such data collection.

## Lifecycle Phase:

The development of a new System of Records (SOR) or modification of an existing SOR is initiated during the Acquisition Phase. The SOR continues to be enhanced during the Requirements Analysis Phase and is subsequently finalized during the Design & Engineering Phase. The completed SOR is subsequently processed through a formal review and clearance process also performed during the Design & Engineering Phase. For information regarding the review process, see Review of System of Records (SOR).

## Guidance:

For information regarding the format and content of the Narrative Statement that is submitted to the Office of Management & Budget (OMB), see:

[System of Records \(SOR\) Narrative Statement Template \(Word Version\)](#)

[System of Records \(SOR\) Narrative Statement Template \(PDF Version\)](#)

For information regarding the format and content of the Preamble and the Statement of Records Notice that are provided to Congress and printed in the *Federal Register*, see:

[System of Records \(SOR\) Preamble and Statement of Records Notice Template \(Word Version\)](#)

[System of Records \(SOR\) Preamble and Statement of Records Notice Template \(PDF Version\)](#)

For additional guidance in the development of the System of Records (SOR) package, contact [OIS/EDG/DDLD](#).

# Computer Match Agreement (CMA)

## Summary Description:

A Computer Match Agreement (CMA) is a written compact that establishes the conditions, safeguards, and procedures under which CMS agrees to disclose data where there is a computerized comparison of two or more automated Systems of Record (SORs). A "matching program" is any computerized comparison of two or more SORs, or a SOR with non-Federal records for the purpose of (1) establishing or verifying eligibility or compliance with law or regulations of applicants or recipients/beneficiaries, or (2) recouping payments or overpayments. The definition also encompasses matches involving Federal personnel or payroll records. In conjunction with a CMA, an Inter/Intra-agency Agreement (IA) is also prepared when the SOR(s) involved in the comparison are the responsibility of another Federal agency.

## Status:

**Conditionally Mandatory - Investment Management Level Deliverable** - All IT projects (Levels B, C and D) must prepare a Computer Match Agreement (CMA) when any computerized comparison of two or more System of Records (SORs) will occur. This also encompasses matches involving Federal personnel or payroll records. In conjunction with a CMA, an Inter/Intra-agency Agreement (IA) is also prepared when the SOR(s) involved in the comparison are the responsibility of another Federal agency.

## Lifecycle Phase:

A Computer Match Agreement (CMA), as well as an associated Inter/Intra-agency Agreement (IA) if necessary, is initiated and completed during the Design & Engineering Phase based on the conditions described above. The completed CMA, and the associated IA if necessary, is subsequently processed through a formal review and clearance process during the Design & Engineering Phase. For information regarding the CMA and IA review processes, see Review of Computer Match Agreement (CMA) or Review of Inter/Intra-agency Agreement (IA).

## Guidance:

For information regarding the preparation of a Computer Match Agreement (CMA), contact OIS/EDG/DDLD.

# Inter/Intra-agency Agreement (IA)

## Summary Description:

An Inter/Intra-agency Agreement (IA), also known as a reimbursable agreement, is a written compact in which a Federal agency agrees to provide to, purchase from, or exchange with another Federal agency services, supplies, or equipment. An IA is the document with which the receiving agency agrees to reimburse the providing agency for the cost of the services, supplies, or equipment. In certain cases two or more agencies may agree to exchange services, supplies, or equipment without a transfer of funds. Although IAs are usually between two agencies, on occasion, they may involve more than two agencies.

1. Intra-agency agreements are between two or more agencies within the Department of Health and Human Services (DHHS).
2. Inter-agency agreements are between at least one component within DHHS and another Federal agency or component outside DHHS.
3. Cost-reimbursement agreements are funds paid for actual charges incurred.
4. Less-than-cost are funds paid that were less than the total cost incurred.
5. No-charge means that no funds were paid for the said exchange identified in the IA.
6. Reciprocal are equal fund amounts paid towards the total cost of a project funded by two or more Federal agencies.

## Status:

**Conditionally Mandatory - Investment Management Level Deliverable** - All IT projects (Levels A, B, C and D) must prepare an Inter/Intra-agency Agreement (IA) in order to provide to, purchase from, or exchange with another Federal agency services, supplies, or equipment.

## Lifecycle Phase:

An Inter/Intra-agency Agreement (IA) is initiated and completed during the Design & Engineering Phase. The completed IA is subsequently processed through a formal review and clearance process also performed during the Design & Engineering Phase. For information regarding the review process, see Review of Inter/Intra-agency Agreement (IA).

## Guidance:

For an electronic copy of the template for an Inter/Intra-agency Agreement for CMS Payables, see:  
[Inter/Intra-agency Agreement \(IA\) Payable Template \(Word Version\)](#)  
[Inter/Intra-agency Agreement \(IA\) Payable Template \(PDF Version\)](#)

For an electronic copy of the template for an Inter/Intra-agency Agreement for CMS Receivables, see:  
[Inter/Intra-agency Agreement \(IA\) Receivable Template \(Word Version\)](#)  
[Inter/Intra-agency Agreement \(IA\) Receivable Template \(PDF Version\)](#)

For guidance in the preparation of an Inter/Intra-agency Agreement (IA), contact [OICS/AGG](#).

# Implementation Readiness Review (IRR) Data Sheet

## Summary Description:

The Implementation Readiness Review (IRR) Data Sheet is a document that signals the completion of activities required prior to production implementation. The IRR Data Sheet is to be made available to all points of contact prior to the IRR so that all parties are aware of what is to be addressed.

## Status:

**Mandatory - Investment Management Level Deliverable** - All CMS IT Systems (Project Levels A, B, C and D) must complete an IRR Data Sheet.

## Lifecycle Phase:

The IRR Data Sheet is initiated and completed at the end of the Implementation Phase. The IRR Data Sheet serves as input to the Implementation Readiness Review (IRR) also performed during the Implementation Phase.

## Guidance:

For an electronic copy of the template and instructions for completing the IRR Data Sheet, see:  
[IRR Data Sheet Template \(Word Version\)](#)  
[IRR Data Sheet Template \(PDF Version\)](#)

For additional guidance in the completion of the IRR Data Sheet, contact [OIS/PMSG/DIS](#).

# System Security Plan (SSP)

## Summary Description:

The System Security Plan (SSP) is a document that provides an overview of the security requirements of the system, describes controls in place to meet those requirements and delineates responsibilities and expected behavior of all individuals who access the system.

## Status:

**Mandatory - Investment Management Level Deliverable** - All IT Projects (Levels A, B, C and D) must complete a System Security Plan (SSP).

## Lifecycle Phase:

The development of a System Security Plan (SSP) is initiated during the Requirements Analysis Phase. The SSP continues to be enhanced throughout the Design & Engineering Phase and the Development Phase, and is subsequently finalized during the Testing Phase. The SSP serves as input to the System Security Plan (SSP) Certification and System Security Plan (SSP) Accreditation performed during the Implementation Phase, as well as input to the System Security Plan (SSP) Re-Certification and System Security Plan (SSP) Re-Accreditation performed during the Operations & Maintenance Phase.

## Guidance:

For an electronic copy of the template for preparing a System Security Plan (SSP), see:  
[System Security Plan \(SSP\) Template \(Word Version\)](#)  
[System Security Plan \(SSP\) Template \(PDF Version\)](#)

For additional guidance in the development of a System Security Plan (SSP), contact [OIS/SSG](#).

# System Security Plan (SSP) Certification Form

## Summary Description:

The System Security Plan (SSP) Certification Form is the form that documents the System Security Plan (SSP) Certification or Re-Certification by the System Owner/Manager, the System Maintainer, and the Component Information Systems Security Officer (ISSO) for a General Support System (GSS), Major Application (MA), or "Other" system.

## Status:

**Mandatory - Investment Management Level Deliverable** - All CMS IT Systems (Project Levels A, B, C and D) must complete a System Security Plan (SSP) Certification Form.

## Lifecycle Phase:

A System Security Plan (SSP) Certification Form is initiated and completed during the Implementation Phase to document the System Security Plan (SSP) Certification. A SSP Certification Form is also completed during the Operations & Maintenance Phase to document the System Security Plan (SSP) Re-Certification.

## Guidance:

For an electronic copy of the template for the System Security Plan (SSP) Certification Form, see:  
[System Security Plan \(SSP\) Certification Form Template \(Word Version\)](#)  
[System Security Plan \(SSP\) Certification Form Template \(PDF Version\)](#)

For additional guidance in the completion of the System Security Plan (SSP) Certification Form, contact [OIS/SSG](#).

# System Security Plan (SSP) Accreditation Form

## Summary Description:

The System Security Plan (SSP) Accreditation Form is the form that documents the System Security Plan (SSP) Accreditation or Re-Accreditation by the CMS Chief Information Officer (CIO), or Senior Management Official Designee (currently the Senior Systems Security Advisor) for a General Support System (GSS), Major Application (MA), or "Other" system to process in the operational environment and to accept the risk associated with it.

## Status:

**Mandatory - Investment Management Level Deliverable** - All CMS IT Systems (Project Levels A, B, C and D) must complete a System Security Plan (SSP) Accreditation Form.

## Lifecycle Phase:

A System Security Plan (SSP) Accreditation Form is initiated and completed during the Implementation Phase to document the System Security Plan (SSP) Accreditation. A SSP Accreditation Form is also completed during the Operations & Maintenance Phase to document the System Security Plan (SSP) Re-Accreditation.

## Guidance:

For an electronic copy of the template for the System Security Plan (SSP) Accreditation Form, see:  
[System Security Plan \(SSP\) Accreditation Form Template \(Word Version\)](#)  
[System Security Plan \(SSP\) Accreditation Form Template \(PDF Version\)](#)

For additional guidance in the completion of the System Security Plan (SSP) Accreditation Form, contact [OIS/SSG](#).