System Security Plan (SSP) Template Instructions

This template contains boiler plate language. Each template must be customized to specifically address the System. Specific System data shall be entered in the template when a colon symbol is indicated. Enter data to the right of the colon symbol. (Example – System Name: Security CBT). When a table is used enter the Response Data to the right of the subject information or the next row under the table column headings. Delete this page prior to the submission of the System SSP.

Office/Center Name and Acronym:
Group Name (acronym):
Centers for Medicare & Medicaid Services

DOCUMENT TITLE:

SSP Date:
SSP Version Number:

SSP Template May 7, 2009 Version 3.1

TABLE OF CONTENTS

SUMMARY OF CHANGES IN THE SSP TEMPLATE V 3.1

1. This document replaces the *CMS System Security Plan Template*, v3.0, dated March 19, 2009.
2. Based on CMS user utilization of v3.0 of the Template, some subsections in Section 2 System Identification, were modified to allow the entry of data without entering the data into a pre-defined tabular format.
3. Modified Section 2.9 System Security Level to reflect "Information Type" in the System Security Description column.
4. Based on CMS user utilization of v3.0 of the Template, some subsections in Section 3 Security Controls Details and Comments, were modified to allow the entry of data without entering the data into a pre-defined tabular format.
5. Subsections in Section 4 Appendices and Attachments were modified to allow the entry of data without entering the data into a pre-defined tabular format.
6. The version number of the document was increased to version 3.1.

REVIEW LOG

This SSP Review Log is maintained to record the reviews that have taken place for this system.
The review log should be completed by entering the data from each column in the appropriate row. The log may also be completed by using a pen.

Date of Review.	Staff Name of Reviewer	Organization of Reviewer

1. INTRODUCTION

The SSP documents the current level of existing security controls within the System that protect the confidentiality, integrity and availability (CIA) of the system and its information.

2. SYSTEM IDENTIFICATION

2.1 SYSTEM NAME / TITLE

System Identifier	Response Data
Official System Name:	
System Acronym:	
System of Records (SOR):	
Financial Management Investment Board (FMIB) Number:	
Select one System Type from the following: - GSS, GSS sub-system, MA or MA individual application	

2.2 RESPONSIBLE ORGANIZATION

CMS Internal	Response Data
Name of Organization:	
Address:	
City, State, Zip:	
Contract Number:	
Contract Name:	

External	Response Data
Name of Organization:	
Address:	
City, State, Zip:	
Contract Number, Contractor contact information (if applicable):	

2.3 DESIGNATED CONTACTS

Business Owner	Response Data
Name:	
Title:	
Organization:	
Address:	
Mail stop:	
City, State, Zip:	
E-Mail:	
Phone Number:	
Contractor contact information (if applicable):	

System Developer/Maintainer	Response Data
Name:	
Title:	
Organization:	
Address:	
Mail stop:	
City, State, Zip:	
E-Mail:	
Phone Number:	
Contractor contact information (if applicable):	

SSP Author	Response Data
Name:	
Title:	
Organization:	
Address:	
Mail stop:	
City, State, Zip:	
E-mail:	

SSP Author	Response Data
Phone Number:	
Contractor contact information (if applicable):	

2.4 ASSIGNMENT OF SECURITY RESPONSIBILITY

Individual[s] Responsible for Security	Response Data
Name:	
Title:	
Organization:	
Address:	
Mail stop:	
City, State, Zip:	
E-mail:	
Phone Number:	
Emergency Contact (daytime): (name, phone & email)	

Component ISSO	Response Data
Name:	
Title:	
Organization:	
Address:	
Mail stop:	
City, State, Zip:	
E-mail:	
Phone Number:	
Emergency Contact (daytime): (name, phone & email)	

2.5 SYSTEM OPERATIONAL STATUS

System Operational Status	Response Data
Select one System Operational Status from the following: New, Operational, or Undergoing a Major Modification.	

2.6DESCRIPTION OF THE BUSINESS PROCESS

The description of the Business Process is provided in this section.

2.7 DESCRIPTION OF OPERATIONAL/SYSTEM ENVIRONMENT AND SPECIAL CONSIDERATIONS

The description of the Operational/System Environment and any Special Considerations are provided in this section.

2.8SYSTEM INTERCONNECTION / INFORMATION SHARING

The description of the System Interconnection/Information Sharing is provided in this section.

2.9SYSTEM SECURITY LEVEL

System Security Description	Response Data
Security Level:	
Information Type:	

2.10 E-AUTHENTICATION LEVEL

Choose the appropriate E-Authentication level for the System/Application and enter the Response Data.

E-Authentication Levels (indicate only one)	Response Data
System/Application has web-based access for individuals to conduct transactions:	
RACF/Top Secret/Active Directory or equivalent is used to authenticate individuals for all web-based transactions:	
No web-based transactions by individuals (proceed to section 3):	

Determine the required level of e-Authentication assurance, based on the impacts of an authentication error, as 1, 2, 3 or 4.

E-Authentication Assurance Levels (indicate only one)	Response Data
Select one E-Authentication assurance level type from the following: Type 1, Type 2, Type 3 or Type 4.	

2.11 APPLICABLE LAWS OR REGULATIONS

The descriptions of the Applicable Laws or Regulations are provided in this section.

2.12 RULES OF BEHAVIOR (ROB)

The descriptions of the Rules of Behavior are provided in this section.

2.13 REVIEW OF SECURITY CONTROLS

The descriptions of the Security Controls Reviewed are provided in this section.

2.14 RISK ASSESSMENT AND RISK MANAGEMENT

The Risk Assessment (RA) and Risk Management (RM) log should be completed by entering the data from each column in the appropriate row

RA Vulnerability	RA Risk Level	RA Recommended Safeguard	RA Residual Risk	RM Status of Safeguard	RM Updated Risk

The description of the Risk Assessment and Risk Management additional information is provided in this section.

2.15 PLANNING FOR SECURITY IN THE SDLC

The description of the Planning for Security in the SDLC is provided in this section.

3 SECURITY CONTROLS DETAIL AND COMMENT

3.1 ACCESS CONTROL (AC) FAMILY

The description of AC security control detail and comments are provided in this section.

3.2 AWARENESS AND TRAINING (AT) FAMILY

The description of AT security control detail and comments are provided in this section.

3.3 AUDIT AND ACCOUNTABILITY (AU) FAMILY

The description of AU security control detail and comments are provided in this section.

3.4 CERTIFICATION, ACCREDITATION AND SECURITY ASSESSMENTS (CA) FAMILY

The description of CA security control detail and comments are provided in this section.

3.5 CONFIGURATION MANAGEMENT (CM) FAMILY

The description of CM security control detail and comments are provided in this section.

3.6 CONTINGENCY PLANNING (CP) FAMILY

The description of CP security control detail and comments are provided in this section.

3.7 IDENTIFICATION AND AUTHENTICATION (IA) FAMILY

The description of IA security control detail and comments are provided in this section.

3.8 INCIDENT RESPONSE (IR) FAMILY

The description of IR security control detail and comments are provided in this section.

3.9 MAINTENANCE (MA) FAMILY

The description of MA security control detail and comments are provided in this section.

3.10 MEDIA PROTECTION (MP) FAMILY

The description of MP security control detail and comments are provided in this section.

3.11 PHYSICAL AND ENVIRONMENTAL PROTECTION FAMILY (PE) FAMILY

The description of PE security control detail and comments are provided in this section.

3.12 PLANNING (PL) FAMILY

The description of PL security control detail and comments are provided in this section.

3.13 PERSONNEL SECURITY (PS) FAMILY

The description of PS security control detail and comments are provided in this section.

3.14 RISK ASSESSMENTS (RA) FAMILY

The description of RA security control detail and comments are provided in this section.

3.15 SYSTEM AND SERVICES ACQUISITION (SA) FAMILY

The description of SA security control detail and comments are provided in this section.

3.16 SYSTEM AND COMMUNICATIONS PROTECTION (SC) FAMILY

The description of SC security control detail and comments are provided in this section.

3.17 SYSTEM AND INFORMATION INTEGRITY (SI) FAMILY

The description of SI security control detail and comments are provided in this section.

3.18 E-AUTHENTICATION (EA) FAMILY

The description of EA security control detail and comments are provided in this section.

4 APPENDICIES AND ATTACHMENTS

APPENDIX A - EQUIPMENT LIST
The description of the Equipment List is provided in this section.

APPENDIX B - SOFTWARE LIST
The description of the Software List is provided in this section.

APPENDIX C – DETAILED CONFIGURATION SETTINGS
The descriptions of the Detailed Configuration Settings are provided in this section.

APPENDIX D - GLOSSARY
The description of the Glossary is provided in this section.

APPENDIX E - ACRONYMS & ABBREVIATIONS
The descriptions of the Acronyms & Abbreviations are provided in this section.

ATTACHMENT 1 (if needed)

The description of the contents of Attachment 1 (if needed) is provided in this section.

ATTACHMENT 2 (if needed)

The description of the contents of Attachment 2 (if needed) is provided in this section.

End of Document