Restricted Distribution
Sensitive Information – For Official Use Only

Centers for Medicare & Medicaid Services

ACA System Security Plan Template

Version 1.0

August 1, 2012

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.

Exchange Name:
System Name & Acronym:

DOCUMENT TITLE:

SSP Date:
SSP Version Number:

TABLE OF CONTENTS

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

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 System Name: **SSP Date and Version Number:**

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

SSP System Name: **SSP Date and Version Number:**

Component ISSO	Response Data
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.	

2.6 DESCRIPTION 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.

2.8 SYSTEM INTERCONNECTION / INFORMATION SHARING

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

2.9 SYSTEM 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	Response Data
Select the E-Authentication assurance level type from the following: Type 1, Type 2, Type 3 or Type 4.	

The description of the authentication mechanism in place to meet the E-Authentication assurance levels identified above.

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.

3. SECURITY CONTROLS DETAIL AND COMMENT

The SSP and SPR coupled together provide the comprehensive control requirements that must be documented for the protection of all data received, stored, processed and transmitted by the health insurance exchanges and data services hub for implementation of the ACA legislation. Security controls common to both CMS and IRS requirements are documented in the SSP. Security controls specific to the protection of FTI or requirements above the common control baseline must be documented in the SPR. Together, the SSP and SPR form the description of the controls in place to protect all data contained in health insurance exchange and data services hub systems – both FTI and non-FTI.

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 INFORMATION SECUIRTY PROGRAM PLAN (PM) FAMILY

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

3.19 ADDITIONAL CONTROLS REQUIRED BY IRS PUBLICATION 1075

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

4. APPENDICES AND ATTACHMENTS

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 supports 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 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.

ATTACHMENT 1 System Security Plan (SSP) Workbook

Controls common to both CMS and IRS requirements are documented in the SSP. In the SSP Workbook, the agency must fully explain how the control or requirement will be implemented.

ATTACHMENT 2 IRS Safeguard Procedures Report (SPR)

Controls specific to the protection of federal tax information (FTI) or requirements above the common controls must be documented in the SPR. Together, the SSP and SPR form the description of all data – both FTI and non-FTI.

End of Document