



**CENTERS for MEDICARE & MEDICAID SERVICES**
Enterprise Information Security Group
7500 Security Boulevard
Baltimore, Maryland 21244-1850

**Workbook:**

# System Security Plan (SSP) Workbook

**FINAL**
**Version 1.5**
**July 31, 2012**

**(This Page Intentionally Blank)**

## SUMMARY OF CHANGES IN E-AUTHENTICATION WORKBOOK, VERSION 4.0, JULY 31, 2012

1. Updated to reflect Changes in CMS *Acceptable Risk Safeguards* manual, Version 1.5.
2. Removed Appendices A, B, and C for ARS control workbooks. Replaced with direction to enter information into the CMS FISMA Controls Tracking System (CFACTS).

## SUMMARY OF CHANGES IN E-AUTHENTICATION WORKBOOK, VERSION 1.0, AUGUST 31, 2010

1. Modified guidance to mandate the full explanation of the control implementation rather than a simple statement of compliance or non-compliance.
2. Restarted Version Number to version 1.0 to be compliant with CMS *Office of Strategic Operations and Regulatory Affairs (OSORA)* manual numbering requirements for the associated CMS *Acceptable Risk Safeguards* manual.

## SUMMARY OF CHANGES IN E-AUTHENTICATION WORKBOOK, VERSION 4.0, NOVEMBER 11, 2009

1. Initial publication started at version 4.0 to synchronize with *CMS Acceptable Risk Safeguards* manual.

**(This Page Intentionally Blank)**

## TABLE OF CONTENTS



## APPENDICES



## LIST OF TABLES

**(This Page Intentionally Blank)**

# 1 INTRODUCTION

## 1.1 CONTROLS WORKBOOKS

The intent of these workbooks is to serve as a tool for the Business Owner or the individual designated in determining the implemented level of compliance with required controls.

The *System Security Plan (SSP) Workbook* ("Workbook") is a resource to be utilized as a part of the overall System Security Plan (SSP) and Information Security (IS) Risk Assessment (RA) development efforts at the Centers for Medicare & Medicaid Services (CMS).

Associated workbooks for control implementation (Appendices A, B, and C) have been superseded. Instead, all control implementation information is to be documented in the CMS FISMA Controls Tracking System (CFACTS) in accordance with procedures published in Volume II of the CMS *Risk Management Handbook (RMH)*.

## 1.2 E-AUTHENTICATION WORKBOOKS

The E-authentication Workbooks (Appendices D through G) are a resource to be utilized as part of the overall SSP and IR SA development efforts when there is a need to remotely authenticate users. The Workbooks provide the user with a list of security procedures that represent the minimum E-authentication controls required for the applicable system. The E-authentication controls are based on the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63, *Electronic Authentication Guideline* and those included in the CMSRs. When there is a difference in the NIST SP 800-63 and the CMSRs, the CMSRs take precedence.

The workbooks address all four (4) levels of assurance for E-authentication and have been developed into two aspects *Registration and Identity Proofing* and *Authentication Mechanism Requirements* that correspond to the four system assurance levels. Level 1 affords little or no confidence in asserted identity's validity, level 2 provides some confidence in asserted identity's validity, level 3 provides high confidence in asserted identity's validity, and level 4 provides very high confidence in asserted identity's validity. The system asserted identity validity level is commensurate with the CMSRs. The level of assurance of the system is driven by the guidance provided in the *ARS* Appendix D. Once the level of assurance has been ascertained, the corresponding Workbook or Appendix (D, E, F, or G) in this document should be utilized. The Workbook contains the expected minimum E-authentication implementation procedures relative to the level of assurance of the system, as mandated by the NIST SP 800-63 and CMSRs. If applicable, the Workbook shall be completed thoroughly, and in its entirety, as a part of the overall SSP and IS RA effort as the information documented in the Workbook shall be used to populate the SSP and IS RA and serve as the evidence in support of any audit activities.

# 2 WORKBOOK INSTRUCTIONS

This section contains instructions on how to complete the appropriate appendix of the Workbooks. The tables below contain the data elements within each Workbook appendix. Each workbook contains the requirements language for use in generating required information necessary to properly generate an SSP and IS RA. Each workbook must be customized to specifically address the specified system. Specific system data shall be entered in the workbook 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, or below the subject information under the appropriate table column or row headings. Delete the applicable appendix cover page prior to completion of the workbook. The applicable SSP workbook is required to be completed as an attachment to all SSPs.

## 2.1 E-AUTHENTICATION WORKBOOK

E-authentication levels are established in accordance with the directions located in the *System Security Levels by Information Type* document posted on the CMS Information Security web site located at http://www.cms.hhs.gov/InformationSecurity. E-authentication workbooks are required to be complete for all systems where e-authentication is applicable. The applicable workbook shall be attached to the SSP.

Table 1 illustrates how the E-authentication workbooks are filled-in. Each of the cells from Table 1 will be explained in Table 2. Additional instructions for filling-in the Workbook forms are provided following the tables.

**Table 1 E-authentication Workbook Design**

| Section Description |
|---|
| E-authentication requirement high-level description |
| **Level X.Y – Second-level Requirement** |
| **Control**<br>E-authentication Requirement |
| **State Compliant or Explain why – Partially Compliant, Non-Compliant or Not Applicable:** |
| **Level X.Y.Z – Third-level Requirement** |
| **Control**<br>E-authentication Requirement |
| **State Compliant or Explain why – Partially Compliant, Non-Compliant or Not Applicable:** |
| **E-authentication Assurance Level Security Controls detail and Comment** |
| Detailed Comments |

**Table 2 E-authentication Workbook Data Elements**

| Data Element | Definition Explanation |
|---|---|
| Section Description | This row (purple) is the section description based upon the E-authentication standards described in the ARS. |
| Level X.Y – Second-level Requirement | This row (brown) is the requirement description based upon the E-authentication standards described in the ARS. This is a pre-filled row. It may or may not be followed by a Control element, depending on whether there is a third- level requirement depth of coverage for this requirement. |
| Level X.Y.Z – Third-level Requirement | This row (orange) is the requirement description based upon the E-authentication standards described in the ARS. This is a pre-filled row. |
| Control | This is the actual controls requirement from the ARS and E-authentication standards. |
| State *Compliant* or Explain why – Partially Compliant, Non-Compliant or Not Applicable Control: Security Requirement with Implementation Standard | **User entered data:** This row must indicate that the control is compliant (C), or why a particular control is Partially Compliant (PC), Non-Compliant (NC) or Not Applicable (NA). Requires a textual response. |
| E-authentication Assurance Level Security Controls Details and Comments | **User entered data:** At the end of each of the E-authentication Workbooks there is a section to amplify and summarize the status for that E-authentication level of assurance. This should be completed *after* all the control items for that level of assurance is are completed. |

# 3 INSTRUCTIONS FOR THE SSP AND RA

The information contained within these workbooks is used to complete the SSP and the RA.

## 3.1 SYSTEM SECURITY PLAN

The SSP template includes a section titled *Security Controls Detail and Comment*. The section includes documenting the implementation of CMS security control requirements for each of the seventeen security control families and the E-authentication assurance level.

When applicable, it is acceptable for the author to copy and paste the information documented within the row titled *Controls Detail and Comment*, at the end of each system family in the applicable Workbook, into the SSP template.

Note - The details and comments contained within the completed SSP, as well as the applicable Security Requirements SSP Workbook (provided as an attachment to the SSP), will be considered the information of record for the description of implemented security controls for the system.

## 3.2 INFORMATION SECURITY RISK ASSESSMENT

The partially compliant and non-compliant controls documented within the workbook are to be identified as threats and documented within the IS RA. Necessary corrective actions should be identified in the applicable *Plan of Actions and Milestones (POA&M)*.

The information documented within the explanation row of the workbook shall be documented in the Risk description.

Information on the existing Risk Determination table shall be referenced from the explanation row and the row titled *Controls Detail and Comment* within the applicable Workbook.

When applicable, it is acceptable for the author to copy and paste the information documented within the row titled *Controls Detail and Comment* from the applicable Workbook into the IS RA template.

# 4 APPROVED

teresa.fryer@cms.hhs.gov

Digitally signed by teresa.fryer@cms.hhs.gov
DN: cn=teresa.fryer@cms.hhs.gov
Date: 2012.08.02 13:57:38 -04'00'

Teresa Fryer
CMS Chief Information Security Officer and
Director, Enterprise Information Security Group

*This document will be reviewed periodically, but no less than annually, by the Enterprise Information Security Group (EISG), and updated as necessary to reflect changes in policy or process. If you have any questions regarding the accuracy, completeness, or content of this document, please contact the EISG at* mailto:ciso@cms.gov*.*

**(This Page Intentionally Blank)**