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

Enterprise Information Security Group

Risk Management, Oversight, And Monitoring

Risk Management Handbook
Volume II
Procedure 2.6

Information System Description

FINAL
Version 1.0
September 14, 2012

Document Number: CMS-CISO-2012-vII-pr2.6

(This Page Intentionally Blank)

SUMMARY OF CHANGES IN *INFORMATION SYSTEM DESCRIPTION*, VERSION 1.0, SEPTEMBER 14, 2012

1. Baseline Version.

(This Page Intentionally Blank)

TABLE OF CONTENTS

(This Page Intentionally Blank)

1 INTRODUCTION

1.1 PURPOSE

The purpose of this procedure is to provide the appropriate personnel with the necessary procedures for successfully addressing the Information System Description. This procedure is necessary to:

- Document the *Information System Description* into CFACTS.
- Describe the information system's data communications, components, ownership, and connections/interconnections.
- Enable the Business Owner (Information System Owner) to ensure accurate development, monitoring, and accountability throughout the system's lifecycle.

1.2 BACKGROUND

The *Information System Description* process is performed and repeated at various stages during a system's lifecycle. During the initiation phase, the Business Owner must identify the need for the information system, to include the business processes the system will support. It is the overall responsibility of the Business Owner to ensure procurement, development, integration, modification, operation, maintenance, and disposal of the Information System.

1.3 OTHER RELEVANT PROCEDURES

Other relevant procedures include:

- RMH Volume II, Procedure 1.1, *Accessing the CFACTS*. This procedure is required to gain an account to, and log into CFACTS.
- RMH Volume II, Procedure 2.3, *Categorizing an Information System*. This procedure describes the process for Security Categorization of an information system in CFACTS.
- RMH Volume II, Procedure 4.2, *Documenting Security Controls in CFACTS*. This procedure provides detailed instructions for properly documenting security controls into CFACTS, which is a requirement for multiple portions of the Information System Description.
- RMH Volume II, Procedure 5.6, *Documenting SCA in CFACTS*. This procedure describes the security control testing and assessment data entry into CFACTS, and also provides the relevant Security Authorization and Assessment (SA&A) data necessary for the Information System description.

All applicable RMH procedures and tools are available in the Info Security Library section on the *CMS Information Security* website: http://www.cms.hhs.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html.

2 PROCEDURES

PROCEDURE	PRINCIPLE
2.1 CREATING OR UPDATING SYSTEM INFORMATION IN CFACTS	
2.1.1 PROCEDURE USERS	
1. CMS Business Owner. 2. CMS Information System Security Officer (ISSO). 3. Business Partner SSO. 4. Designated CFACTS data entry person.	
2.1.2 INITIAL CONDITIONS	
1. The information system exists in CFACTS.	
a. If not, contact the CISO mailbox for a *CFACTS General Information Intake Form* and complete as directed.	*Contact the EISG at* mailto:ciso@cms.hhs.gov.
2. User has authorized access to applicable CMS system in CFACTS.	
a. Refer to RMH Volume II, Procedure 1.1, *Accessing the CFACTS*, for further guidance on gaining authorized access to CFACTS.	

PROCEDURE	PRINCIPLE
2.1.3 ESTABLISHING OR UPDATING SYSTEM INFORMATION IN CFACTS	
2.1.3.1 ESTABLISHING OR UPDATING GENERAL AND/OR DETAILED INFORMATION IN CFACTS	
1. For the *General Information* tab information in CFACTS, perform the following:	
a. Complete the *CFACTS General Information Intake Form*.	Available at *http://www.cms.hhs.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html*.
b. Submit the *CFACTS General Information Intake Form* to CMS CISO mailbox.	Submit to *mailto:ciso@cms.hhs.gov.*
2. Log into CFACTS using RMH Volume II, Procedure 1.1, *Accessing the CFACTS*.	
3. Click on the link for the applicable system from either the *Home* screen or the *Browse* Screen.	*Opens the applicable system to the* Identification *tab.*
4. On the *System Identification* tab, select the *Detailed Description* radio button.	*Displays the* Detailed Description *view of the* System Identification *screen.*
5. For the *Operating Location* field, list ALL of the geographic locations where this system (or any and all of its components) are housed.	*Include all CMS data centers, contractor sites, or cloud providers where any portion of the system is operating. This field should also reflect the "system boundary" as described in the SSP and other supporting system security documentation.*

PROCEDURE	PRINCIPLE
6. For the *Prepared By* field, enter the name of the POC responsible for performing this procedure.	
7. For the *Purpose* field, describe the business objectives and purpose of this system.	
8. If a specialized *Logo* exists for the system, perform the following to update or load a logo:	*A logo file must be a graphic (JPEG, PNG, or BMP) file type.*
a. If a file is already listed in the *Logo* field:	
(1) In the *Logo* field, click on the *Delete* link.	*Removes the listed file and returns to the* Identification *screen.*
b. In the *Logo* field, click on the *Upload* link.	
c. Click on the *Browse* button and select the *logo* graphic file.	
d. Click on the *Upload* button.	*Uploads the applicable logo file.*
e. Click on the *Close* button.	*Returns to the* Identification *screen.*
9. If specialized diagrams or graphics exist for the system, perform the following to load or update:	*An image file must be a graphic (JPEG, PNG, or BMP) file type.*
a. To add a *New* image file:	
(1) In the *Environment Details* field, click on the *New* link.	*Opens the* Add Description *screen.*
(2) In the *Title* field, type in a short *Title* for the image.	
(3) In the *Description* field, type in a *Description* for the image.	
(4) Click on the *Save* button.	*Returns to the* Identification *screen.*
(5) For the newly added image, click on the applicable *Upload* link.	
(6) Click on the *Browse* button and select the applicable graphic file.	
(7) Click on the *Upload* button.	*Uploads the applicable logo file.*

PROCEDURE	PRINCIPLE
(8) Click on the *Close* button.	*Returns to the* Identification *screen.*
b. To edit a file *Title* or *Description*:	
(1) For the applicable image, click on the *Edit* link.	Opens the Add Description screen.
(2) In the *Title* field, type in a new *Title* for the image.	
(3) In the *Description* field, type in a new *Description* for the image.	
(4) Click on the *Save* button.	*Returns to the* Identification *screen.*
c. To change or update an existing image file:	
(1) For the applicable image, click on the *Upload* link.	
(2) Click on the *Browse* button and select the applicable graphic file.	
(3) Click on the *Upload* button.	*Uploads the applicable logo file.*
(4) Click on the *Close* button.	*Returns to the* Identification *screen.*
d. To *Delete* an existing image file:	
(1) For the applicable listed image file, click on the *Delete* link.	*Removes the listed file and returns to the* Identification *screen.*

2.1.3.2 ESTABLISHING OR UPDATING SYSTEM SECURITY CATEGORY IN CFACTS

1. Declare or update system security category in accordance with the *Completing the Security Categorization Worksheet* procedure in RMH Volume II, Procedure 2.3, *Categorizing an Information System*.

PROCEDURE	PRINCIPLE
2. EISG staff updates the information in CFACTS in accordance with the *Determine the Security Category* procedure in RMH Volume II, Procedure 2.3, *Categorizing an Information System*.	
2.1.3.3 ESTABLISHING OR UPDATING CAPITAL PLANNING INFORMATION IN CFACTS	
1. Log into CFACTS using RMH Volume II, Procedure 1.1, *Accessing the CFACTS*.	
2. Click on the link for the applicable system from either the *Home* screen or the *Browse* Screen.	*Opens the applicable system to the* Identification *tab.*
3. On the *System Identification* tab, select the *Capital Planning* radio button.	*Displays the* Capital Planning *view of the* System Identification *screen.*
4. For the *OMB Exhibit* field, select the appropriate investment planning *OMB Exhibit*.	
5. For the *UII* field, perform ***one*** of the following:	
a. If a *Unique Investment Identifier (UII)* has been assigned, enter it in the *UII* field, ***or***	Unique Investment Identifier (UII) *is a persistent numeric code applied to an investment that allows the identification and tracking of an investment across multiple fiscal years of an agency's investment portfolio. The unique investment identifier is composed of a 3-digit agency code concatenated with a 9-digit unique investment number generated by the agency.*

PROCEDURE	PRINCIPLE
b. If ***no*** *UII* has been assigned, enter the legacy *Unique Project Identifier (UPI)* code.	Unique Project Identifier (UPI) *means the identifier depicting agency code, bureau code, part of the Exhibit 53 where investment will be reported, mission area, type of investment, agency four-digit identifier, and two-digit investment category code used to report the investment in any previous Exhibit 53 submission to OMB. Indicating the UPI used for a previous submission allows cross-walk and historical analysis crossing fiscal years for tracking purposes.*
6. For the *Investment Name* field, type the appropriate *Investment Name* from the applicable planning Exhibit.	
CAUTION: **Do not enter a dollar value in the following two fields. Contractors who have access to CFACTS should not be exposed to this information.**	
7. For the current year *IT spending* field, **ONLY enter $0.00**.	*Do not enter a dollar value. Contractors who have access to CFACTS cannot be exposed to this data.*
8. For the following year *projected IT spending* field, **ONLY enter $0.00**.	*Do not enter a dollar value. Contractors who have access to CFACTS cannot be exposed to this data.*

2.1.3.4 ESTABLISHING OR UPDATING PEOPLE AND INVENTORY IN CFACTS

1. Log into CFACTS using RMH Volume II, Procedure 1.1, *Accessing the CFACTS*.	
2. Click on the link for the applicable system from either the *Home* screen or the *Browse* Screen.	*Opens the applicable system to the* Identification *tab.*
3. On the *Identification* screen, click on the *People and Inventory* Tab.	

PROCEDURE	PRINCIPLE
4. Select the *POCs* radio button.	*Displays the* POCs *view of the* People and Inventory *screen.*
5. Create or verify that, at a minimum, a correct POC entry exists for the *Business Owner*, *System Developer/Maintainer*, and *Information Systems Security Officer (ISSO).*	Business Owners *are CMS federal employees who are at the Group Director level or above;* System Developer/Maintainers *are CMS federal employees who are at the Division Director level or above;* ISSOs *are CMS federal employees who are on the CMS ISSO list (https://www.cms.hhs.gov/cbt/downloads/isso_list.pdf) maintained by EISG.*
6. If any of the POC entries listed above are missing or incorrect, perform the following for each applicable POC:	*A system must have at least a Business Owner, System Developer/Maintainer, and Information System Security Officer (ISSO).*
a. To create or update a POC:	
(1) Perform one of the following:	
(a) Click on the *New* link, ***or***	*Opens the* Add Information Point of Contact *screen.*
(b) Click on the *Edit* link for the applicable POC.	*Opens the* Edit Information Point of Contact *screen.*
(2) In the *Name* field, enter/update the full *Name* of the applicable POC.	
(3) In the *SA&A Role* field, select/ update the applicable *SA&A Role* of the applicable POC from the dropdown list.	
(4) In the *HR Title* field, enter/update the applicable *HR Title* of the applicable POC.	
(5) In the *Component* field, enter/ update the CMS business *Component* of the applicable POC.	*For contractors, enter the* Company *name.*
(6) In the *Address* field, enter/update the full mailing *Address* of the applicable POC.	*For CMS employees, include any applicable* Mail Stop.
(7) In the *Phone* field, enter/update the business *Phone* number of the applicable POC.	

PROCEDURE	PRINCIPLE
(8) In the *Email* field, enter/update the full *Email* address of the applicable POC.	
(9) In the *Receive Email Notifications* field, select *Yes* or *No* from the dropdown list to receive email notification sent to POCs for the applicable system.	
(10) In the *Fax* field, enter/update the *Fax* number of the applicable POC.	
(11) In the *Responsibility* field, describe/update the SA&A *Responsibilities* of the applicable POC.	
(12) Click on the *Save* Button.	*Saves information and returns to the* POCs *view of the* People and Inventory *screen.*
(13) To add/update additional POCs, return to step (1) (a)	*For contractors, add applicable contractor security personnel (such as SSO) and other applicable CFACTS data-entry and security personnel.*
b. To *Delete* an existing POC, click on the *Delete* link for the applicable POC, then click on *Yes* to confirm.	*Returns the user to the* POCs *view of the* People and Inventory *screen.*

2.2 ESTABLISHING OR UPDATING "GENERAL" SYSTEM INFORMATION IN CFACTS

2.2.1 PROCEDURE USERS

1. EISG Staff.

2.2.2 INITIAL CONDITIONS

1. The information system exists in CFACTS.

PROCEDURE	PRINCIPLE
2. User has authorized access to applicable CMS system in CFACTS.	*Requires* EISG Support *user role.*
3. EISG has received the *CFACTS General Information Intake Form* from applicable BO or ISSO.	
2.2.3 ESTABLISHING OR UPDATING "GENERAL" SYSTEM INFORMATION	*Only EISG Staff have the necessary access rights to perform this procedure.*
1. Log into CFACTS using RMH Volume II, Procedure 1.1, *Accessing the CFACTS.*	
2. Select, or verify selected, the *General Information* radio button.	*Displays the* General Information *view of the* Identification *screen.*
3. For the *Contractor Operation of Facility* field, perform ***one*** of the following:	
a. Select, or verify selected, ***No*** if the system is *completely* housed and hosted within ***CMS Baltimore Enterprise Data Center***, **or**	*Select **No** if the system is* wholly *housed **ONLY** within the* **CMS Baltimore Enterprise Data Center**.
b. Select, or verify selected, ***Yes*** for ***all*** others.	
4. For the *Program* field, leave as *Not Applicable* unless specifically directed by EISG management.	
5. For the *Site* field, leave as *Not Applicable* unless specifically directed by EISG management.	
6. For the *Parent System* field, leave as *Not Applicable* unless specifically directed by EISG management.	
7. For the *Acronym* field, leave as currently populated unless specifically directed by EISG management.	*This field is matched with enterprise architecture data maintained at HHS, and cannot be changed without coordination with HHS.*
8. For the *Number of Users* field, enter the approximate number of users for this system.	

PROCEDURE	PRINCIPLE
9. For the *System Type* field, select the appropriate *System Type* from the dropdown.	
10. For the *This System is an Operational Network* field, leave as *No* unless specifically directed by EISG management.	
11. For the *Financial System* field, leave as currently populated unless specifically directed by EISG management.	Financial Systems *are managed and accounted for as a specific subset of FISMA systems under the CFO Act, and have additional accounting and reporting requirements beyond non-financial systems.*
12. For the *Is Critical Asset* field, leave as *No* unless specifically directed by EISG management.	Critical Assets *are managed and accounted for as a specific subset of CMS systems under the Federal Continuity Directive 1 (FCD 1), dated February 2008, and have additional management, recovery, and reporting requirements beyond non-critical assets.*
13. For the *SDLC Status* field, select, or verify selected, the appropriate *SDLC Status*, from the dropdown list.	
14. For the *Creation Date* field, leave as populated by CFACTS.	
15. Click on the *Save* button.	

3 APPROVED

teresa.fryer@cms.hhs.gov

Digitally signed by teresa.fryer@cms.hhs.gov
DN: cn=teresa.fryer@cms.hhs.gov
Date: 2012.10.22 09:15:03 -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.hhs.gov.

(This Page Intentionally Blank)