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

Risk Management Handbook
Volume II
Procedure 2.3

Categorizing an Information System

FINAL
Version 1.2
April 23, 2013

Document Number: CMS-CISO-2013-vII-proc2.3

(This Page Intentionally Blank)

SUMMARY OF CHANGES IN CATEGORIZING AN INFORMATION SYSTEM VERSION 1.2, DATED APRIL 23, 2013

1. Reworded step 5 of section 2.1.3 because the security category is now displayed when the form is complete.

SUMMARY OF CHANGES IN CATEGORIZING AN INFORMATION SYSTEM VERSION 1.2, DATED SEPTEMBER 10, 2012

1. Renamed references and hyperlinks to the Information Security Library throughout the document.

SUMMARY OF CHANGES IN CATEGORIZING AN INFORMATION SYSTEM VERSION 1.0, DATED JULY 17, 2012

1. Baseline Version.

(This Page Intentionally Blank)

TABLE OF CONTENTS

1 OVERVIEW 1

1.1 Purpose 1

1.2 Other Relevant Procedures and Tools 1

2 INFORMATION SYSTEM CATEGORIZATION PROCEDURE 2

2.1 Completing the Security Categorization Worksheet 2

2.1.1 Procedure Users 2

2.1.2 Initial Conditions 2

2.1.3 Security Categorization Worksheet Procedure 3

2.2 Determine the Security Category 4

2.2.1 Procedure Users 4

2.2.2 Initial Conditions 4

2.2.3 Security Categorization procedure 5

3 APPROVED 8

(This Page Intentionally Blank)

1 OVERVIEW

1.1 PURPOSE

The purpose of this procedure is to provide appropriate personnel, with various specified information system security responsibilities, the necessary procedures to:

- Describe the type(s) of information the system will process, store, access, or transmit in sufficient detail to enable determination of the security category of the information system, using the *Security Categorization Worksheet*.
- Document the information type(s) in CFACTS, which determines the security category.
- Upload the *Security Categorization Worksheet* to CFACTS.

1.2 OTHER RELEVANT PROCEDURES AND TOOLS

Other relevant procedures and tools include:

- RMH Volume II, Procedure 1.1, *Accessing the CFACTS*. This procedure is required to gain access to, and log into the CFACTS.
- Tool: *System Categorization Worksheet*. This worksheet enables gathering all information that is necessary to determine the security category of the information system.

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

2 INFORMATION SYSTEM CATEGORIZATION PROCEDURE

PROCEDURE	PRINCIPLE
2.1 COMPLETING THE SECURITY CATEGORIZATION WORKSHEET	
2.1.1 PROCEDURE USERS	
1. CMS Business Owners. 2. System Developers/Maintainers. 3. CMS Information System Security Officer (ISSO). 4. CFACTS EISG Support.	
2.1.2 INITIAL CONDITIONS	
1. A new system is conceived.	*When ideas for a new system or changes to an existing system occur, there is usually sufficient information regarding the type(s) of information the final system will process to accurately determine the security category of that system.*
2. A change to an existing system is conceived.	

PROCEDURE	PRINCIPLE
2.1.3 SECURITY CATEGORIZATION WORKSHEET PROCEDURE	
1. Download and save the Tool - *System Categorization Worksheet* from the *Information Security Library*, http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html.	*Always download a copy of the worksheet to ensure you use the current version of the document.*
2. Open the saved *System Categorization Worksheet*.	*Microsoft Excel will open the worksheet.* ***NOTE:*** *Cell B1 says, "Form is NOT completed." This message will remain until all required information has been entered.*
3. Enter the name of the information system and its abbreviation in cell B2.	*For example: Wonderful New System (WNS).*
4. For each of the rows 5 through 15:	
a. Read the *Description of Information* in column B and determine if the system will process, store, access, or transmit any information of the applicable type.	
(1) If the system will ***process***, ***store***, ***access***, or ***transmit*** any information of this type enter an X in the *Yes* column (column C) for the applicable row.	
(2) Otherwise, enter an X in the *No* column (column D) for the applicable row.	
5. If cell B1 does ***NOT*** state the system security category and indicate the information type(s) that determined it.	
a. Re-perform steps 3 and 4 to complete the form.	

PROCEDURE	PRINCIPLE
NOTE: **The following steps must be performed by the CMS Business Owner.**	
6. Sign the *System Categorization Worksheet* by adding the Business Owner**'s** digital signature.	*The signature block is located at the bottom of the worksheet.* *Note: The method to digitally sign a document in Microsoft Excel differs among versions. Use Excel help to determine the appropriate method for your version.*
7. Save the *System Categorization Worksheet.*	
8. Send a copy of the completed and digitally signed *System Categorization Worksheet* for the applicable system to the EISG at mailto:ciso@cms.gov. In the email subject line, type: *Security Categorization Request for [System Name]*.	Contact the IT Help Desk if you need help regarding digitally signing a document.

2.2 DETERMINE THE SECURITY CATEGORY

2.2.1 PROCEDURE USERS

1. EISG Staff

2.2.2 INITIAL CONDITIONS

1. The information system is registered in CFACTS.

2. User has authorized access to the applicable CMS system in CFACTS.

Contact the EISG at mailto:ciso@cms.gov with questions regarding user roles and their access limits.

a. Refer to RMH Volume II, Procedure 1.1, *Accessing the CFACTS*, for further guidance on gaining authorized access to CFACTS.

PROCEDURE	PRINCIPLE
3. User has a completed, digitally signed, and EISG-approved *System Categorization Worksheet* from the applicable business owner.	*The worksheet is the source of information needed to determine the security category of the system. The signature indicates the content of the worksheet is accurate and has not been changed without business owner approval.*
2.2.3 SECURITY CATEGORIZATION PROCEDURE	
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. Click on the *FIPS 199* radio button.	*Opens the* FIPS 199 *view.*
4. In the *Security Categorization* section, click on *Security Categorization Wizard* link.	*This opens the Security Categorization Wizard, which displays a list of the information types that the information system accesses, stores, processes, or transmits.*
5. For each *Information Type* in the *System Categorization Worksheet* perform the following steps:	
a. For each *Information Type* marked as ***No***:	
(1) If the applicable *Information Type* appears within the list of information types in the CFACTS *Security Categorization Wizard*:	
(a) Delete the applicable *Information Type* from CFACTS.	

PROCEDURE	PRINCIPLE
b. For each *Information Type* marked as ***Yes***:	
(1) If this *Information Type* does ***not*** appear in the list of information types in the CFACTS *Security Categorization Wizard*:	*Opens the* Information Security Categorization *entry form.*
(a) Click on *New*.	
(b) For the *Component Name* field, select *CMS*.	
(c) For *Management/Support Line of Business* field, select *Security Levels.*	
(d) Select the *Information Type* that matches the applicable *Information Type* in column A of the current row of the *System Categorization Worksheet*.	
(e) Click on the *Save* button.	
(f) Click on the *Close* button.	*Returns the user to the* List of Information Types *window. The new information type should now appear.*
(g) Return to Step (1) and re-perform until each applicable *Information Types* has been addressed.	
c. When all *Information Types* have been processed, click on the *Close* button of the *List of Information Types* screen.	*Returns the user to the* FIPS 199 *view. The appropriate* Security Category *should now be indicated.*
6. Click on the *SA&A Tracking* tab.	
7. In the *Miscellaneous* section of the *SA&A Tracking* tab, perform the following:	*The* Miscellaneous *section is at the bottom of the* SA&A Tracking *screen.*
a. Update the *System Categorization Date* field to reflect the date that the *System Categorization Worksheet* was digitally signed.	

PROCEDURE	PRINCIPLE
b. If there is no document loaded in the *1 position* of the *Miscellaneous* section:	*If there are no supporting documents uploaded for* FIPS 199*, the first (topmost) row of the* Num *column will be blank. If a document has already been loaded, there should be a* 1 *in the first position of the* Num *column.*
(1) Click the *Upload* link for the first row.	*This opens the document upload window.*
c. If there is a document loaded in the 1 position of the Miscellaneous section:	
(1) Click the *New* link.	
d. Select *FIPS* as the document type.	
e. In the *Title* field, type the *Date*, *Title*, and *initials* of the Business Owner/signer of the *System Categorization Worksheet*.	*Example: "02/28/2012, FIPS 199, (XXX)"* *Where (XXX) are the initials of the person who digitally signed the worksheet.*
f. Click on the *Browse* button and select the applicable *System Categorization Worksheet*.	
g. Click the *Upload* button.	
h. Click the *Close* button.	*Return the user to the* SA&A Tracking *tab.*
i. Move the new *FIPS 199* document to the *1* (topmost) *position* as follows:	
(1) Within the *Miscellaneous* section, click on the *Move* link.	*This opens a document sequence control screen for Miscellaneous Artifacts.*
(a) In the *From Artifact Position* field, select from the dropdown the document just uploaded in the steps above.	
(b) In the *To Artifact Position* dropdown field, select *1 – [Old document title]*.	
(c) Click on the *Save* button, then click on *OK* to confirm the move.	
8. On the *SA&A Tracking* screen, click 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: 2013.04.25 11:32:49 -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.