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 7.8
Key Updates

FINAL
Version 1.0
August 17, 2012

Document Number: CMS-CISO-2012-vII-pr7.8

(This Page Intentionally Blank)

SUMMARY OF CHANGES IN KEY UPDATES VERSION 1.0, DATED AUGUST 17, 2012

1. Baseline Version.

(This Page Intentionally Blank)

TABLE OF CONTENTS

(This Page Intentionally Blank)

1 INTRODUCTION

1.1 PURPOSE

The purpose of the *Key Updates Procedure* is to facilitate the near real-time management of risk associated with the operation and use of each information system. This requires having and maintaining information regarding the current: implementation of security controls, effectiveness of implemented controls, vulnerabilities within the information system or its environment of operation, and repair status of identified vulnerabilities; as well as current risks to the information system, mission/business process and CMS. The *Key Updates Procedure* is performed continuously, once a system starts operation.

1.2 BACKGROUND

By law, each CMS FISMA system must obtain an Authority to Operate (ATO) before it is placed into operation. This requires that security controls be operational, effective, managed, and continuously monitored. Controls must meet mandatory requirements, as defined in the current *CMS Information Security Acceptable Risk Safeguards (ARS) CMS Minimum Security Requirements (CMSR).*

Additional security controls may be implemented to lower the risk associated with the use and operation of an individual information system. Such additional controls usually arise from unique mission/business process needs to control the level of certain risks to CMS, the mission/business process, the system itself or its environment of operation. These controls must also be operational, effective, managed, and continuously monitored.

Information in CFACTS forms the basis to know the risk associated with the use and operation of the system at any point in time. This information must be current, credible, accurate, complete, and in accordance with published CMS procedures. The processes that keep information current can be time-driven (e.g., once a week or every 365 days), event-driven (e.g., changes to the system or its environment of operation, personnel changes, business process changes, discovery of new vulnerabilities, or a weakness remediation is completed), or both time-driven and event-driven. The *Key Updates* procedure deals with updates that are event-driven.[1] Three examples of changes that often result in event-driven updates are:

- Modification of security controls based on risk mitigation activities of the system owner or common control provider, such as when the weakness status becomes closed in the POA&M management process.
- Detection of a weakness in control effectiveness found through continuous monitoring or a security control assessment.
- Revision of the *CMS Information Security Acceptable Risk Safeguards (ARS), CMS Minimum Security Requirements (CMSR).*

[1] Time driven updates are addressed using RMH Volume II, Procedure 6.3, *Security Information Review* at the time intervals specified by the *CMS Minimum Security Requirements (CMSR)*.

1.3 HOW TO USE THIS PROCEDURE

The *Key Updates Procedure* is broken into two columns: *Procedure* and *Principle*. The Procedure column specifically addresses the necessary steps to perform in order to complete the process. The Principle column provides additional information about the procedure to aid understanding.

1.4 RELATED PROCEDURES

Other relevant *Risk Management Handbook (RMH)* procedures include:

- RMH Volume I, Chapter 1, *Risk Management in the XLC*. This chapter provides information required to understand the interrelation of information security, risk management, the CMS Expedited Life Cycle (XLC), and the system life cycle.
- RMH Volume II, Procedure 1.1, *Accessing the CFACTS*. This procedure is required to gain access to, and log into the CFACTS.
- RMH Volume II, Procedure 2.3, *Categorizing an Information System.* This procedure is required to establish the system's security category in CFACTS.
- RMH Volume II, Procedure 2.6, *Information System Description.* This procedure is required to create or update system information in CFACTS.
- RMH Volume II, Procedure 4.2, *Documenting Security Controls in CFACTS*. This procedure is required to document security controls in CFACTS and is a prerequisite for documenting testing of the applicable security control(s).
- RMH Volume II, Procedure 5.6, *Documenting Security Control Effectiveness in CFACTS*. This procedure is required to document security control testing, and directs the documentation of identified weaknesses.
- RMH Volume II, Procedure 6.2, *POA&M Management*. This procedure is required to ensure that *Weaknesses* are properly documented and managed in CFACTS.
- RMH Volume II, Procedure 6.3, *Security Information Review*. This procedure is required to ensure that all information in CFACTS is accurate, complete, credible, current, and in accordance with published CMS procedures.

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

2 PROCEDURES

PROCEDURE	PRINCIPLE
2.1 KEY UPDATES	
2.1.1 PROCEDURE USERS	
1. CMS Information System Security Officer (ISSO). 2. Business Partner System Security Officer (SSO). 3. Designated CFACTS data entry person.	
2.1.2 INITIAL CONDITION	
1. User has authorized access to the applicable CMS system in CFACTS.	*Refer to RMH Volume II, Procedure 1.1,* Accessing the CFACTS, *for further guidance on gaining authorized access to CFACTS.*
2. A change occurred that might affect the accuracy, completeness, or timeliness of information in CFACTS regarding the security state or risks of operating and using the system.	
2.1.3 KEY UPDATES PROCEDURE	*It is important to update relevant information. However, only update relevant information.*
1. Review the change that happened and determine what, if any, specific CFACTS information should undergo review and, if appropriate, update.	*Example: closure of a weakness often relates to a specific security control description or risk item, which could require updates. However, unless the weakness specifically relates to contingency planning an update to the contingency plan is unlikely.*

PROCEDURE	PRINCIPLE
NOTE: **If the change involves storing, processing, accessing, or transmitting any Personally Identifiable Information (PII), by or through a system that did not previously store, process, access, or transmit PII, the change is considered *Significant* and this procedure does not apply. The system will require a new ATO to address the change.**	*All steps and tasks of the Risk Management Framework must be performed following RMH Volume I, Chapter 1,* Risk Management in the XLC.
2. Review the *Privacy Impact Assessment (PIA)* as follows*:*	*Any major change to the data that result in privacy risks shall be accurately reflected in the PIA.*
a. Evaluate to determine if the data associated with the system has been affected by any of the following factors:	
(1) Conversions of *form.*	*A conversion from paper-based methods to electronic systems.*
(2) *Anonymous to non-anonymous*.	*The system's function, as applied to an existing information collection, changes anonymous information into PII;*
(3) Significant *system management* changes.	*In the case that new uses of an existing IT system, including application of new technologies, significantly change the process of managing PII in the system;*
(4) Significant *merging*.	*When agencies adopt or alter business processes so that government databases holding PII are merged, centralized, matched with other databases, or otherwise significantly manipulated;*
(5) New *public access*.	*When user-authenticating technology (e.g., password, digital certificate, biometric) is newly applied to an electronic information system, which can be accessed by the public;*
(6) *Commercial* sources.	*PII, obtained from commercial or public sources, is systematically integrated into the existing information system's database;*

PROCEDURE	PRINCIPLE
(7) New *interagency* uses.	*When agencies work together on shared functions involving significant new uses or exchanges of PII;*
(8) Internal *flow* or *collection.*	*When alteration of a business process results in significant new uses or disclosures of information, or incorporation into the system of additional PII; and*
(9) Alteration in *Character* of data.	*When new PII added to a collection raises the risks to personal privacy, such as the addition of health or privacy information.*
b. If changes to any of the above factors has occurred, immediately contact the *CMS Privacy Office* to determine if an *update* to the *PIA* and/or *SORN(s)* is required.	*If any of these or other scenarios occur, each affected section within the PIA shall be updated to reflect the current state of the information system. For PIA questions, contact the Privacy Office at mailto:pia@cms.gov.*
NOTE: **If the system processes additional information types, which result in the system having a different security category, the change is *Significant* and this procedure does not apply. The system will require a new ATO to address the change.**	*All steps and tasks of the Risk Management Framework must be performed following RMH Volume I, Chapter 1,* Risk Management in the XLC.
3. Review the *System Categorization Worksheet* as follows:	
a. Obtain the current worksheet from 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) Click on the *Security Authorization* tab.	

PROCEDURE	PRINCIPLE
(4) In the *Miscellaneous* section of the *Security Authorization* tab, perform the following:	*The* Miscellaneous *section is at the bottom of the* SA&A Tracking *screen.*
(a) If a current FIPS 199 document is not loaded into position *Num* 1 of the documents table proceed immediately to step c.	*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.*
(b) Click on the name of the current FIPS 199 document in the first row under the column entitled *Support Document* and choose open to view the System Categorization Worksheet.	*This opens the document in Microsoft Excel.*
b. Review all information in the System Categorization Worksheet for correctness.	
(1) If all information is correct, proceed to step 4.	
c. Update the *System Categorization Worksheet* and submit it in accordance with RMH Volume II, Procedure 2.3, *Categorizing an Information System.*	
4. Review the *Information System Description as follows:*	*Any major change to the data that result in privacy risks shall be accurately reflected in the PIA.*
a. Evaluate to determine if the data associated with the system has been affected by any factors, including:	
(1) Personnel changes.	
(2) Changes to system functionality.	
(3) Equipment changes.	
(4) Software changes.	
(5) Processing location changes.	
(6) New user populations.	
(7) New system interfaces.	

PROCEDURE	PRINCIPLE
(8) Network changes. b. If there are changes to any *Information System Description* factors, including those listed above, update CFACTS in accordance with RMH Volume II, Procedure 2.6, *Information System Description,* using the *Creating or Updating System Information in CFACTS procedure* for the affected information.	
5. Review the *system boundary* as follows:	*Any major change to the data that result in privacy risks shall be accurately reflected in the PIA.*
a. Evaluate to determine if the system boundary has been affected by any factors, including: (1) Contractor changes. (2) Configuration changes. (3) Equipment changes. (4) Software changes. (5) Processing location changes. (6) New user populations. (7) New system interfaces. (8) Telecommunications methods or vendor changes. (9) Network changes. b. If there are changes to any *system boundary* factors, including those listed above, update CFACTS in accordance with *CMS System Security Plan (SSP) Procedure,* section 3.1.1 and the portion of Appendix A (page 29) entitled "Boundary Issues."	

PROCEDURE	PRINCIPLE
6. If the change relates to the implementation of security controls or revisions to security control requirements, update the security control description for each affected control requirement in accordance with RMH Volume II, Procedure 4.2, *Documenting Security Controls in CFACTS.*	*Examples of related changes are closure of a weakness and an update to* CMS Information Security Acceptable Risk Safeguards (ARS), CMS Minimum Security Requirements (CMSR).
7. Review the business and information system risk tables as follows:	*Any major change to the data that result in privacy risks shall be accurately reflected in the PIA.*
a. Evaluate to determine if the business or information system risk are affected (raised or lowered) by any factors, including:	
(1) Closure of a weakness.	
(2) Changing equipment, configurations, software, or processing locations.	
(3) New or changed system functionality.	
(4) Personnel and contractor changes.	
(5) Change in communications methods or vendors.	
(6) New user populations.	
(7) New system interfaces.	
(8) Audit and assessment findings.	
(9) Annual attestation control testing.	
(10) Continuous monitoring results.	
(11) Security incidents.	
(12) Use of new technology.	
(13) New (or changed) missions or business processes.	

PROCEDURE	PRINCIPLE
b. If there are changes to any business or information system risk factors, including those listed above, update CFACTS in accordance with *CMS Information Security Risk Assessment (IS RA) Procedure*, sections 4.3, 4.4 and the portion of Appendix A (pages 36-38) entitled Risks And Safeguards Table.	
8. Review the contingency planning information as follows:	
a. Evaluate to determine if the contingency planning information associated with the system has been affected by any of the following factors:	*Changes in mission and business process requirements.*
(1) Evaluate to determine if the *Maximum Tolerable Disruption (MTD)* for the business has changed since the last *Contingency Plan* update.	*The MTD is the maximum time a business can tolerate the absence or unavailability of a particular business function. This includes the maximum time for restoring the IT systems,* ***plus*** *the additional time (not associated with recovering the information technology) necessary to recover the* business *back to a normal state. (MTD=RTO+WRT [see below])*
(2) Evaluate to determine if the *Recovery Time Objective (RTO)* for the system has changed since the last *Contingency Plan* update.	*The RTO is the maximum time a business function can be disrupted/not available before it causes serious and irreversible impact.*
(3) Evaluate to determine if the *Recovery Point Objective (RPO)* for the system has changed since the last *Contingency Plan* update.	*The RPO is the amount or extent of data loss that can be tolerated by your business functions. For instance, If a system fails, how much data loss can the business tolerate (that might result from recent data collected but not backed-up, thus not recovered)?*

PROCEDURE	PRINCIPLE
(4) Evaluate to determine if the *Work Recovery Time (WRT)* for the business has changed since the last *Contingency Plan* update.	*The WRT is the time it takes to get critical* business *functions back up and running once the systems (hardware, software, and configuration) are restored to the RPO. This includes the manual processes necessary to verify that the system has been restored to the RPO, and all necessary processes have been completed to address the remaining lost, or out-of-synch, data or business processes.*
(5) Evaluate to determine if personnel or contractor changes have occurred since the last *Contingency Plan* update.	
(6) Evaluate to determine if system operation procedures have changed since the last *Contingency Plan* update.	
(7) Evaluate to determine if backup procedures, media, or services have changed since the last *Contingency Plan* update.	
b. If changes to any of the above factors have occurred, update the *Contingency Plan* in accordance with *CMS Information Security Contingency Plan (CP) Procedures*.	
9. If *Contingency Plan Test* results indicate the need for change to *Contingency Plan* content, update the *Contingency Plan* in accordance with *CMS Information Security Contingency Plan (CP) Procedures*.	

3 APPROVED

teresa.fryer@cms.hhs.gov

Digitally signed by teresa.fryer@cms.hhs.gov
DN: cn=teresa.fryer@cms.hhs.gov
Date: 2012.08.17 09:19:01 -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)