CMS
CENTERS for MEDICARE & MEDICAID SERVICES

Office of the Chief Information Security Officer
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

OCISO
OFFICE OF THE CHIEF INFORMATION SECURITY OFFICER
Risk Management, Oversight, And Monitoring

Risk Management Handbook
Volume II
Procedure 6.2

POA&M Management

FINAL
Version 1.00
February 13, 2012

Document Number: CMS-CISO-2012-vII-pr6.2

(This Page Intentionally Blank)

SUMMARY OF CHANGES IN POA&M MANAGEMENT VERSION X.X

1. Baseline Version.

(This Page Intentionally Blank)

TABLE OF CONTENTS

(This Page Intentionally Blank)

1 OVERVIEW

1.1 PURPOSE

The purpose of this procedure is to provide the security personnel with CFACTS data entry responsibilities the necessary procedures for entering the following information into CFACTS:

- Creating and documenting a new *Weakness* in CFACTS, up to and including the first *Milestone* (indicating that additional *Milestones* must be developed and documented.)
- Creating and documenting new weakness *Milestones* in CFACTS, including all necessary actions for each *Milestone* required to fully-remediate the identified weakness.
- Updating applicable *Weakness* statuses on a monthly basis for all active *Weaknesses*.

1.2 OTHER RELEVANT PROCEDURES

Other relevant procedures include:

- 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 4.2, *Documenting Security Controls in CFACTS*. This procedure requires that security controls be properly documented in CFACTS as a prerequisite for documenting *Weaknesses* and POA&M remediation in CFACTS
- RMH Volume II, Procedure 5.6, *Documenting Security Control Effectiveness in CFACTS*. This procedure is a likely source of weaknesses identified, and directs the documentation of weaknesses to this procedure.
- RMH Volume II, Procedure 7.3, *CMS Annual Attestation Procedure* relies on this procedure to ensure that POA&M information is current as a prerequisite for submitting an annual attestation.

All applicable RMH procedures are available on the CMS information Security website, in the *Info Security Library* at: http://www.cms.gov/InformationSecurity/ISD/list.asp.

2 PLAN OF ACTIONS AND MILESTONES (POA&M) PROCEDURE

PROCEDURE **PRINCIPLE**

2.1 DOCUMENTING A WEAKNESS IN CFACTS

2.1.1 PROCEDURE USERS

1. CMS ISSO.

2. Business Partner SSO.

3. Designated CFACTS data entry person.

4. OCISO Staff.

2.1.2 INITIAL CONDITIONS

1. User has entered this procedure after being directed ***by another procedure*** to document a weakness.

For example, RMH Volume II, Procedure 5.6, Documenting Security Control Effectiveness in CFACTS *refers to this document to document any identified weaknesses.*

2. The *Add Weakness* screen is open on the user’s browser for the applicable system.

2.1.3 DOCUMENTING A WEAKNESS IN CFACTS PROCEDURE

PROCEDURE	PRINCIPLE
1. Ensure that the *Class* field reflects the appropriate class of the ARS control family of the control requirement for which this weakness has been identified.	*CFACTS* ***may*** *pre-assign the* Class (Technical, Operational, *or* Management) *based on the* Class *of a failed control. Depending on from where the* Add Weakness *form was accessed, this information may already be correct as pre-populated. The applicable Classes for families of controls are listed in the ARS and the PISP.*
2. Ensure that the *Family* field reflects the appropriate ARS control family of the control requirement for which this weakness has been identified.	*CFACTS* ***may*** *pre-assign the ARS Control* Family *based on the* Family *of a failed control. Depending on from where the* Add Weakness *form was accessed, this information may already be correct as pre-populated.*
3. For the *Creation Date* field, maintain the *Creation Date* as assigned by CFACTS.	*CFACTS assigns the default* Creation Date *of the current (today's) date. No change is required or desired.*
4. For the *Weakness* field:	
a. DELETE any existing text in this field.	*In some cases, CFACTS* may *insert the word "Deficiency" followed by the full text of the Control Requirement and all applicable Enhancements. CMS does not need or desire this text.*

PROCEDURE	PRINCIPLE
b. Insert the following ***minimum*** information into the *Weakness* description:	*CMS requires the four minimum elements defined in the GAO Yellow Book,* Government Auditing Standards[1]*, to be included in any deficiencies noted.*
(1) The *criteria* for the failed control requirement.	*Discuss which portion of the applicable control* Assessment Procedure *was not met.* *Example: "Failure of AC-2.1 Criteria: Examination of access control policies determined that the organization does not require appropriate approvals for requests to establish accounts, as required in AC-2 baseline requirement in CMS ARS."*
(2) The *condition* for the failed control requirement.	*Discuss the observed situation, as it existed at the time of the assessment.* *Example: "Failure of AC-2.1 Condition: Users are currently granted Admin-level access to the application with only Network-Admin review and authority. No management personnel approve access requests."*
(3) The *cause* for the failed control requirement.	*Discuss the probable reason for this condition existing.* *Example: "Failure of AC-2.1 Cause: The application Business Owner has not developed a documented process for requesting and approving access to various defined user Groups."*

[1] The U.S. Government Accountability Office (GAO) *Government Auditing Standards* (Yellow Book) can be found at http://www.gao.gov/yellowbook.

PROCEDURE	PRINCIPLE
(4) The *effect (or potential effect)* for the failed control requirement.	*Discuss the potential (or real) impact for failing to meet this requirement.* *Example: “Failure of AC-2.1 Effect: Not having an approval process allows a single individual (network Admin) the default authority to grant access to a user, without separate management review of the ‘appropriateness’ of the requested access. This ‘authority’ allows the network-Admin, who is likely not qualified to assess the ‘business need’ of a request, to grant inappropriate access with little or no oversight or review.”*
5. For the *Status* field, maintain the *Status* as *Draft*.	*The OCISO will review and approve weaknesses and corrective action plans. The OCISO will provide the appropriate ISSO feedback in the event the initial milestone is not acceptable by OCISO. If the initial milestone is approved, the OCISO will change the weakness status from “Draft” to “Ongoing”.*
6. For the *Criticality (Priority)* field, select the appropriate *Criticality* from the dropdown.	*The choices from the dropdown will be based on either the source of the weakness or will be a* Management Decision. Unprioritized *is not a desired Criticality (Priority). Higher numbers signify a greater CMS priority for remediating this weakness.* *Example: “2 – Annual Assessment Finding”*
7. For the *Point of Contact* field, include the appropriate *name, phone,* and *email address.*	*Provide information for the person who is best able to address questions on the development and progress tracking of this weakness.*
8. For the *Risk Category* field, select the appropriate *Risk* value for this weakness.	*A security assessor should provide a perceived* Risk *value as part of the assessment. However, if a* Finding *will be linked to this* Weakness, *the* Risk *value MUST be* **at least** *as high as any linked* Finding(s).

PROCEDURE	**PRINCIPLE**
9. For the *Resources Required* field, provide a monetary estimate of the cost of remediating this weakness.	*Estimates should include total costs for implementing the corrective actions for this weakness. (Only input* numbers *in this field.)* *Zero dollars ($0) is* **not** *a valid cost estimate because resources are* ***already being spent*** *just typing in this weakness. All cost, including government and contractor resource person-hours, hardware, and software, should be aggregated into the estimated costs. Additional information that conveys how this estimate will be* funded *is required to be entered later in this procedure.*
10. For the *Severity* field, perform ***one*** of the following:	
a. If the weakness *Risk Category* is *High*, select *Reportable Condition* from the dropdown, ***or***	
b. If the weakness *Risk Category* is *Moderate* or *Low*, select *Other Weakness* from the dropdown.	*OCISO will provide direction if a weakness has been elevated to any other category.*
11. For the *Type* field, maintain the *Type* as assigned by CFACTS.	*CFACTS will assign based on the designation of the* system, site, *or* program.
12. For the *Scheduled Completion Date* field, indicate an estimated *Scheduled Completion Date* to complete ***all*** of the proposed corrective actions.	*This date may be changed while the Weakness is in* Draft *status. However, after the weakness is accepted by OCISO and changed to a* Status *other than* Draft, *this date will become non-editable. Note: The* Estimated Completion Date *(below) will remain editable.*
13. For the *Estimated Completion Date* field, maintain the *Estimated Completion Date* the same as the *Scheduled Completion Date*.	*This date may change throughout the life of the weakness.*
14. For the *Actual Completion Date* field, maintain this field as blank.	*Leave blank until the OCISO approves of the proposed corrective actions. This field will populate when the OCISO approves of the final* closure *of the weakness.*

PROCEDURE	PRINCIPLE
15. For the *Is Material Weakness* field, maintain the *Is Material Weakness* as assigned by CFACTS.	*This field is not editable except by OCISO support staff.*
16. For the *Exclude from OMB Reporting* field, maintain the *Exclude from OMB Reporting* as assigned by CFACTS.	*This field is not editable except by OCISO support staff.*
17. For the *Risk Accepted* field, maintain the *Risk Accepted* as assigned by CFACTS.	*This field is not editable except by OCISO support staff.*
18. For the *Weakness ID* field, maintain the *Weakness ID* as assigned by CFACTS.	*CFACTS will generate and maintain appropriate weakness ID numbers.*
19. For the *Milestone Description* field:	
a. ***DELETE*** any existing text in this field.	*In some cases, CFACTS may insert the word "Deficiency" followed by the full text of the Control Requirement and all applicable Enhancements. CMS does not need or desire this text.*
b. Enter the following text: *"Develop the remaining Milestones necessary to remediate (in-full) all of the elements of this weakness, AND receive CMS OCISO concurrence (within the CFACTS) of the validity of these planned milestones."*	*The* **first** *milestone should* **always** *be to research and determine the necessary remaining milestones required to address the weakness stated above. OCISO will validate and approve these milestones and/or provide additional feedback.*
20. For the *Milestone Scheduled Completion Date* field, enter a date ***no more than*** 33 days from the current date.	
21. Click on the *Save* button.	

PROCEDURE	PRINCIPLE
22. Enter remaining information:	*Several* ***Comment buttons*** *(indicated with the ellipses symbol on the button […]) on the screen become visible after initial* Saving *of a new weakness.*
a. For the *Weakness* field, click on the *comment button* and enter additional comments and any proposed corrective actions from the assessor.	*Depending on from where the* Add Weakness *form was accessed, this information may already be pre-populated with some relevant information.*
b. For the *Point of Contact* field, click on the *comment button* and update as appropriate or enter additional missing information on the *Point of Contact*.	*Depending on from where the* Add Weakness *form was accessed, this information may already be pre-populated with some relevant information.*
c. For the *Resources Required* field, click on the *comment button* and enter:	
(1) The *Funding Source* from the dropdown list.	
(2) Enter any additional *Comments* for the overall funding of the remediation of the weakness.	
NOTE **At least ONE *Control* and/or *Test Number* MUST be associated with each Weakness.**	*Assessors should provide the applicable association within the assessment report. If the associated* Test Number *or* Control *is not provided, the ISSO (or their authorized designate) should establish the applicable association.*
d. For the *Link to Control* field, click on the *comment button* and verify/add the applicable *Control* and/or *Test Number*(s).	*Depending on from where the* Add Weakness *form was accessed, this information may already be pre-populated with some relevant information.*
e. For the *Identified In* field, click on the *comment button* and perform the following steps:	
(1) Add to the *List of Identified In Sources* by clinking on *New*.	

PROCEDURE	PRINCIPLE
(2) If a *Report* has ***not*** already been created:	
(a) Select the *A new Report* radio button.	
(b) Click on the *Next* button.	
(c) In the *Report ID* field type in a report tile that includes the date and type of report.	*Example: "May 2012 - Annual Assessment"*
(d) In the *Report Title* field, enter a short description of the report.	*Example: "2011 Annual Assessment that includes the AT, AU, CP, IR, MA, and PE control families."*
(e) In the *Report Date* field, enter the date that the assessment was completed.	*Example: "05/28/2012"*
(f) In the *Recommendation Number* field, enter the number "1".	
(g) In the *Report Description* field, leave blank.	
(h) Click on the *Save* then *Close* buttons.	
(3) If a *Report* ***has*** already been created:	
(a) Select the *An Existing Report* radio button:	
(b) Click on the *Next* button.	
(c) Select the applicable *Report ID* from the dropdown list.	
(d) Click the *Save* then *Close* buttons.	*Return to the* Edit Weakness *screen.*

PROCEDURE	PRINCIPLE
23. In the *List of Weakness Artifacts* field, upload relevant *Weakness Artifacts as follows:*	
a. Click on *New*.	
b. In the *Title* field, enter the *Weakness ID* followed by a short file *description*.	*Example: "Sys_B_2012_1 - SCAP Data Feed"*
c. Click the *Browse* button and select the applicable file to upload.	
d. Click the *Upload* button.	
e. Click the *Close* button.	*Return to the* Edit Weakness *screen.*
24. Click the *Save* button.	
25. Click the *Close* button.	*Returns to the* Self-Assessment *screen*
26. Perform one of the following:	
a. Add additional *Milestones* in accordance with Section 2.2, *Creating New Weakness Milestones*, ***or***	
b. Return to the calling procedure and perform any remaining steps.	*Return to the procedure that directed the performance of this procedure. Perform any remaining steps in the calling procedure as directed.*

2.2 CREATING NEW WEAKNESS MILESTONES

2.2.1 PROCEDURE USERS

1. CMS ISSO.

2. Business Partner SSO.

PROCEDURE **PRINCIPLE**

3. Designated CFACTS data entry person.

4. OCISO Staff.

2.2.2 ENTRY CONDITIONS

1. Weaknesses already exist in the CFACTS tool.

The weaknesses to be updated must have already been entered into the CFACTS tool. If not, contact the OCISO to determine the status of data entry into CFACTS.

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

You must have an EUA account, been granted access to the CFACTS, and be a designated POC for the applicable system to be updated.

3. The *Edit Weakness* screen is open on the user's browser for the applicable weakness.

2.2.3 CREATING NEW WEAKNESS MILESTONES PROCEDURES

NOTE

If the *Status* of the applicable weakness is anything other than *Draft*, the weakness *Scheduled Completion Date* cannot be modified any further.

In addition, milestones edits and/or modifications are subject to the following rules:
- *Milestone* Scheduled Completion Dates *cannot exist beyond the weakness* Estimated Completion Date
- *Weakness* Estimated Completion Dates *cannot exist beyond the weakness* Scheduled Completion Date *unless the weakness has a* Status *of* Draft, Delayed, Pending Verification, *or* Completed.

1. In the *List of Milestones* field, click on the *New* link.

Opens the Add Milestone *screen.*

2. For the *Milestone Number*, leave as populated by CFACTS.

This number is auto-generated and maintained by the CFACTS application, and cannot be modified.

PROCEDURE	PRINCIPLE
3. For the *Scheduled Completion Date* field, enter the date that the milestone is scheduled to be complete.	*CFACTS will not allow a milestone* Scheduled Completion Date *beyond the weakness* Estimated Completion Date.
4. For the *Milestone Status* field, maintain the status of the milestone as *Not Started*.	
5. For the *Actual Completion Date* field, maintain the *Actual Completion Date* as *TBD*.	*This field must have either a Date or TBD. CFACTS does not allow blank fields.*
6. For the *Point of Contact* field, include the appropriate *name*, *phone*, and *email address.*	*Provide information for the person who is best able to address questions on the development and progress tracking of this milestone.*
7. For the *Milestone* field, enter the following information:	
a. *Title* of the milestone:	*Example: "Create User Roles:"*
b. *Objective* that the milestone is designed to achieve.	*Example: "Objective: Create user roles that properly identify each of the applications user roles and the necessary data access and restriction for each role."*
c. *Method* for how the objective will be achieved.	*Example: "Method: ISSO will interview business owners and/or system developer to determine all of the 'types of users' necessary to access the system, with minimal access rights, to achieve each of the system's functional requirements. From the list of user types, develop the necessary roles, identify the access requirements and restrictions for each role."*
d. *Criteria* for determining when the milestone has been completed.	*Example: "Criteria: This milestone will have been reached when all of the functional requirements can be achieved within the identified and documented roles."*
e. *Next Step* after completion of this milestone.	*Example: "Next Step: When this milestone has been achieved, proceed to milestone 'Develop required Database and Application Roles in code' to integrate the identified roles into the application."*

PROCEDURE	PRINCIPLE
8. For the *Milestone Changes* field, maintain the *Milestone Changes* blank.	
9. Click on the *Save* button.	*Saves and closes the* Add Milestone *screen and returns to the* Edit Weakness *screen.*
10. In the *List of Milestones* field, click on the *Edit* link.	*Opens the* Edit Milestone *screen.*
11. For the *Point of Contact* field, click on the *comment button* and update as appropriate, or enter additional missing information on the *Point of Contact*.	*Several* Comment *buttons (indicated with the ellipses symbol on the button [...]) on the screen become visible after initial* Saving *of a new milestone.*
12. In the *List of Milestone Artifacts* field, upload relevant milestone artifacts as follows:	
a. Click on *New*.	
b. In the *Title* field, enter the *Milestone Number* followed by a short file *description*.	*Example: "Milestone 4 - NESSUS Data Feed"*
c. Click the *Browse* button and select the applicable file to upload.	
d. Click the *Upload* button.	
e. Click the *Close* button.	*Return to the* Edit Weakness *screen.*

2.3 UPDATING WEAKNESS STATUS

This procedure is performed on a monthly basis for all CMS systems.

2.3.1 PROCEDURE USERS

1. CMS ISSO.

2. Business Partner SSO.

3. Designated CFACTS data entry person.

PROCEDURE	PRINCIPLE
4. OCISO Staff.	

2.3.2 ENTRY CONDITIONS

PROCEDURE	PRINCIPLE
1. *Weaknesses* and *Milestones* already exist in the CFACTS tool.	*The weaknesses to be updated must have already been entered into the CFACTS tool.*
2. User has authorized access to the applicable CMS systems in CFACTS.	*You must have an EUA account, been granted access to the CFACTS, and be a designated POC for the applicable system to be updated.*

2.3.3 UPDATING WEAKNESS STATUS PROCEDURES

This procedure should be performed on a monthly basis for each weakness for applicable systems.

PROCEDURE	PRINCIPLE
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 *POA&Ms* tab.	*Opens the* List of Weaknesses *screen.*
4. For each open *weakness* listed, perform the following:	*Open weakness are defined as not* Completed *or* Pending Verification.
a. If the weakness *Status* is ***Draft***, proceed as follows:	
(1) Click on the *Edit* link for the applicable weakness.	*Opens the* Edit Weakness *screen for the applicable weakness.*

PROCEDURE	PRINCIPLE
NOTE: **Do NOT change the *Status* of a weakness from *Draft* to any other *Status*. The OCISO is the only entity authorized to approve and transition a weakness corrective action plan from *Draft*.**	*Once a weakness is promoted from* Draft *to* ***any other*** **Status***, many critical fields become locked and are no longer capable of being edited or updated. If a weakness is promoted from* Draft *inappropriately,* **immediately** *contact the OCISO (at* [*mailto:CISO@cms.gov*](mailto:CISO@cms.gov)*) to transition the weakness back to a* Draft *status.*
(2) Proceed to Section 2.2, *Creating New Weakness Milestones* and verify that all weakness milestones have been developed and documented appropriately.	*For any weaknesses that have been created, ensure that a complete set of appropriate milestones have been developed and documented.*
(3) If a *Plan of Actions & Milestones Review Disposition (PRD)* form has been received from the OCISO, proceed with the instructions included in the PRD for the applicable weakness.	*The PRD form is official feedback from the OCISO POA&M review team that indicates that further ISSO actions are required before the Weakness corrective actions will be approved by the OCISO.*
(4) Click on the *Save* button.	*Saves any changes made on the* Edit Weakness *screen.*
(5) Click on the *Close* button.	*Closes the* Edit Weakness *screen and returns to the* List of Weaknesses *screen.*
(6) Return to Step 4 to address any other weaknesses.	
b. If the ***Status*** is ***Not Started***,	
(1) Click on the *Edit* link for the applicable weakness.	*Opens the* Edit Weakness *screen for the applicable weakness.*
(2) Change the status to *Ongoing*.	
(3) Click on the *Save* button.	*Saves any changes made on the* Edit Weakness *screen.*
(4) Click on the *Close* button.	*Closes the* Edit Weakness *screen and returns to the* List of Weaknesses *screen.*
(5) Return to Step 4 and address this weakness as a status of *Ongoing*.	

PROCEDURE	**PRINCIPLE**
c. If the *Status* is ***Ongoing*** or ***Delayed***,	
(1) Click on the *Edit* link for the applicable weakness.	*Opens the* Edit Weakness *screen for the applicable weakness.*
(2) Ensure that the *Class* field reflects the appropriate class of the ARS control family of the control requirement for which this weakness has been identified.	
(3) Ensure that the *Family* field reflects the appropriate ARS control family of the control requirement for which this weakness has been identified.	
(4) For the *Creation Date* field, maintain the *Creation Date* as assigned by CFACTS.	*This field is locked and cannot be changed.*
(5) Maintain the *Weakness* field as currently maintained in CFACTS. If additional information needs to be added, proceed as follows:	*This field is locked and cannot be changed.*
(a) Click on the *comment button* and.	
(b) Enter additional comments	
(c) Enter any additional proposed corrective actions.	
(d) Click the *Save* button.	
(e) Click the *Close* button.	

PROCEDURE	PRINCIPLE
(6) For the *Status* field, update the *Status* as required to reflect any change to the weakness *Status*. Proceed as follows:	*This status is directly related to the aggregated status of all of the applicable weakness milestones.*
NOTE: **Do NOT change a weakness *Status* to ANY other *Status* other than *Delayed* or *Pending Verification* unless directed by OCISO**	Delayed *or* Pending Verification *are the only authorized choices for non-OCISO users.*
(a) To change to a *Status* of ***Delayed***:	
i. Select a *Status* of *Delayed* from the *Status* dropdown list.	
ii. Click on the comments button for the *Status* field.	*Opens the* Edit Delay Reason *screen.*
iii. From the *Delay Reason* field, select the appropriate reason for the delay in remediating this weakness.	
iv. In the *Comment* field, describe in specific-detail the reason this weakness remediation has been delayed.	
v. Click on the *Save* button.	
vi. Click on the *Close* button.	*Closes the* Edit Delay Reason *screen and returns to the* Edit Weakness *screen.*
(b) To change to a *Status* of ***Pending Verification***:	
i. Select a *Status* of *Pending Verification* from the *Status* dropdown list.	
ii. Update the *Actual Completion Date* field to the *actual* date where this weakness remediation was completed.	

PROCEDURE	PRINCIPLE
(7) For the *Criticality (Priority)* field, update as required the appropriate *Criticality* from the dropdown.	*The choices from the dropdown will be based on either the source of the weakness or will be a* Management Decision. Unprioritized *is not a desired Criticality (Priority). Higher numbers signify a greater CMS priority for remediating this weakness.* *Example: "2 – Annual Assessment Finding"*
(8) For the *Point of Contact* field, click on the *comment button* and enter any additional missing information on the Point of Contact.	*Depending on from where the* Add Weakness *form was accessed, this information may already be pre-populated with some relevant information.*
(9) For the *Risk Category* field, update as required the appropriate *Risk* value for this weakness.	*A security assessor should provide a perceived* Risk *value as part of the assessment. However, if any additional* Findings *will be linked to this* Weakness*, the* Risk *value MUST be* ***at least*** *as high as any linked* Finding(s).
(10) For the *Resources Required* field, update as required the monetary estimate of the cost of remediating this weakness.	*Estimates should include total costs for implementing the corrective actions for this weakness. (Only input* numbers *in this field.)* *Zero dollars ($0) is* **not** *a valid cost estimate because resources are* ***already being spent*** *just typing in this weakness. All cost, including government and contractor resource person-hours, hardware, and software, should be aggregated into the estimated costs. Additional information that conveys how this estimate will be* funded *is required to be entered later in this procedure.*
(11) For the *Resources Required* field, update as required the monetary estimate of the cost of remediating this weakness as follows. (a) Click on the *comment button.* (b) Select the appropriate *Funding Source* from the dropdown list.	

PROCEDURE	**PRINCIPLE**
(c) Enter any additional *Comments* for the overall funding of the remediation of the weakness.	
(d) Click on the *Save* button.	
(e) Click on the *Close* button.	
(12) For the *Severity* field, unless specified by OCISO, maintain this field as *Other Weakness.*	*OCISO will provide direction is a weakness has been elevated to another category.*
(13) For the *Type* field, maintain the *Type* as assigned by CFACTS.	*CFACTS will assign based on the designation of the* system, site*, or* program.
(14) Maintain the *Scheduled Completion Date* field as currently maintained in CFACTS.	*This date will is not editable. Note: The* Estimated Completion Date *(below) is editable.*
NOTE: **The *Estimated Completion Date* cannot be modified beyond the current *Scheduled Completion Date* unless the *Status* is immediately updated to *Delayed*.**	
(15) If the weakness *Estimated Completion Date* must be adjusted, perform the following:	*This date may change throughout the life of the weakness.*
(a) If the *Estimated Completion Date* needs to be adjusted beyond the *Scheduled Completion Date*, perform the following:	
i. Change the weakness *Status* to *Delayed*.	*The* Estimated Completion Date *cannot be modified beyond the current* Scheduled Completion Date *unless the Status is* ***immediately*** *updated to* Delayed.
(b) Modify the *Estimated Completion Date* as required.	

PROCEDURE	PRINCIPLE
(16) For the *Is Material Weakness* field, maintain the *Is Material Weakness* as assigned by CFACTS.	*This field is not editable except by OCISO support staff.*
(17) For the *Exclude from OMB Reporting* field, maintain the *Exclude from OMB Reporting* as assigned by CFACTS.	*This field is not editable except by OCISO support staff.*
(18) For the *Risk Accepted* field, maintain the *Risk Accepted* as assigned by CFACTS.	*This field is not editable except by OCISO support staff.*
(19) For the *Weakness ID* field, maintain the *Weakness ID* as assigned by CFACTS.	*This field is not editable. CFACTS will generate and maintain appropriate weakness ID numbers.*
NOTE **At least ONE *Control* and/or *Test Number* MUST be associated with each Weakness.**	*Assessors should provide the applicable association within the assessment report. If the associated* Test Number *or* Control *is not provided, the ISSO (or their authorized designate) should establish the applicable association.*
(20) For the *Link to Control* field, click on the *comment button* and verify/add the applicable *Control* and/or *Test Number*(s).	
(21) For the *Identified In* field, click on the *comment button* and verify that all applicable sources are listed. If a source is not listed, perform the following steps:	
(a) Click on the *New* link.	
(b) If a *Report* ***has*** already been created:	
i. Select the *An Existing Report* radio button:	
ii. Click on the *Next* button.	

PROCEDURE	**PRINCIPLE**
iii. Select the applicable *Report ID* from the dropdown list.	
iv. Click the *Save* button.	
v. Click the *Close* button.	*Return to the* Edit Weakness *screen.*
(c) If an applicable *Report* has ***not*** already been created:	
i. Select the *A new Report* radio button.	
ii. Click on the *Next* button.	
iii. In the *Report ID* field type in a report tile that includes the date and type of report.	*Example: "May 2012 - Annual Assessment"*
iv. In the *Report Title* field, enter a short description of the report.	*Example: "2011 Annual Assessment that includes the AT, AU, CP, IR, MA, and PE control families."*
v. In the *Report Date* field, enter the date that the assessment was completed.	*Example: "05/28/2012"*
vi. In the *Recommendation Number* field, enter the number "1".	
vii. In the *Report Description* field, leave blank.	
viii. Click on the *Save* then *Close* buttons.	
(22) In the *List of Weakness Artifacts* field, upload any additional *Weakness Artifacts* as follows:	
(a) Click on *New*.	

PROCEDURE	PRINCIPLE
(b) In the *Title* field, enter the *Weakness ID* followed by a short file *description*.	*Example: "Sys_B_2012_1 - SCAP Data Feed"*
(c) Click the *Browse* button and select the applicable file to upload.	
(d) Click the *Upload* button.	
(e) Click the *Close* button.	*Return to the* Edit Weakness *screen.*
(f) Click the *Save* button.	
(g) Click the *Close* button.	*Returns to the* Self-Assessment *screen*
(h) Click on the *Save* button.	*Saves any changes made on the* Edit Weakness *screen.*
(i) Click on the *Close* button.	*Closes the* Edit Weakness *screen and returns to the* List of Weaknesses *screen.*
NOTE: **At least *ONE* milestone for each weakness *MUST* be in a *Status* of *Ongoing* (or *Delayed*) until ALL of the *Milestones* are updated to a *Status* of either *Pending Verification* or *Completed*.**	*Remediation of all known weaknesses must be **actively** pursued, and corrective actions applied as soon as possible. If there are **justifiable** extenuating reasons for a delay in fixing a known issue, risk-mitigating controls **must** be put into effect in the interim and tracked. An applicable milestone must exist for any mitigating interim controls, and the status updated monthly until the* entire *weakness is fully-and-completely remediated.*
(23) For each *Milestone* listed in the *List of Milestones* field, perform the following:	
(a) Click on the *Edit* link.	*Opens the* Edit Milestone *screen.*
(b) Leave the *Milestone Number* as populated by CFACTS.	*This number is auto-generated and maintained by the CFACTS application, and cannot be modified.*
(c) For the *Scheduled Completion Date* field, verify/update the date that the milestone is scheduled to be complete.	*CFACTS will not allow a milestone* Scheduled Completion Date *to exist beyond the weakness* Estimated Completion Date.

PROCEDURE	PRINCIPLE
NOTE:	
Do NOT change a *Milestone Status* to ANY other *Status* other than *Not Started, Delayed* or *Pending Verification* unless directed by OCISO	Not Started, Delayed *or* Pending Verification *are the only authorized choices for non-OCISO users.*
(d) If the *Milestone Status* field is to be changed, update the *Milestone Status* of the milestone as follows:	*Do not change the* Milestone Status *to* Completed. *OCISO will verify that weakness and associated milestone have actually been completed.*
i. Select the applicable *Milestone Status* from the *Milestone Status* dropdown list.	Not Started, Delayed *or* Pending Verification *are the only authorized choices for non-OCISO users.*
ii. Click on the *Milestone Status* field *comment* button.	*Opens the* Edit Status Comment *screen.*
iii. Enter a description for why the *Milestone Status* has been changed.	
iv. Click on the *Save* button.	*Saves and Closes the* Edit Status Comment *screen.*
(e) If the *Milestone Status* has been changed to *Pending Verification*, perform the following:	*Do not change the* Milestone Status *to* Completed. *OCISO will verify that weakness and associated milestone have actually been completed.*
i. Delete any text in the *Actual Completion Date* field.	
ii. Enter the appropriate date for when this milestone was reached.	*This field must have either a Date or TBD. CFACTS does not allow blank fields.*
(f) For the *Point of Contact* field, verify/update the appropriate *name, phone*, and *email address.*	*Provide information for the person who is best able to address questions on the development and progress tracking of this milestone.*
(g) For the *Milestone* field, maintain the *Milestone* description as previously entered.	

PROCEDURE	PRINCIPLE
(h) For the *Milestone Changes* field, describe/update any *Milestone Changes*.	
(i) For *milestones* that are ***Ongoing*** or ***Delayed***, update the *List of Milestone Updates* field by performing the following:	
i. Click the *New* link in the *List of Milestone Updates* field.	*Opens the* New Milestone Status *screen.*
ii. In the *Description* field, describe the progress made in this milestone over the past 30 days.	
iii. In the *% Complete* field, indicate the total percentage towards completion of the applicable milestone.	
iv. Click on the *Save* button.	*Saves the information entered on the* New Milestone Status *screen.*
v. Click on the *Close* button.	*Closes the* New Milestone Status *screen.*
(j) Click on the *Save* button.	*Saves and closes the* Add Milestone *screen.*
(k) In the *List of Milestone Artifacts* field, upload additional relevant milestone artifacts as follows:	
i. Click on *New*.	
ii. In the *Title* field, enter the *Milestone Number* followed by a short file *description*.	*Example: "Milestone 4 - NESSUS Data Feed"*
iii. Click the *Browse* button and select the applicable file to upload.	
iv. Click the *Upload* button.	
v. Click the *Close* button.	*Return to the* Edit Weakness *screen.*

PROCEDURE

(24) Return to Step 4 to address any other weaknesses.

d. If the *Status* is ***Pending Verification***, no action is required this month. Return to Step 4 to address any other weaknesses.

e. If the *Status* is ***Completed***, no further action is required. Return to Step 4 to address any other weaknesses.

5. Exit this procedure.

PRINCIPLE

Within 30 days OCISO will either:

- *Issue a PRD for additional actions*, **or**

- *Update the status to* Completed.

3 APPROVED

teresa.fryer@cms.hhs.gov

Digitally signed by teresa.fryer@cms.hhs.gov
DN: cn=teresa.fryer@cms.hhs.gov
Date: 2012.02.13 15:45:07 -05'00'

Teresa Fryer
CMS Chief Information Security Officer and
Director, Office of the Chief Information Security Officer

This document will be reviewed periodically, but no less than annually, by the Office of the Chief Information Security Officer (OCISO), 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 OCISO at mailto:ciso@cms.gov.

(This Page Intentionally Blank)