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

OFFICE OF THE CHIEF INFORMATION SECURITY OFFICER

Risk Management, Oversight, And Monitoring

Risk Management Handbook
Volume II
Procedure 7.3

CMS Annual Attestation Procedure

FINAL
Version 1.0
February 13, 2012

Document Number: CMS-CISO-2012-vII-pr7.3

(This Page Intentionally Blank)

SUMMARY OF CHANGES IN *CMS ANNUAL ATTESTATION PROCEDURE* VERSION 1.1

1. Updated to address changes to attestation process changes for 2012.

SUMMARY OF CHANGES IN *CMS ANNUAL ATTESTATION PROCEDURE* VERSION 1.0

1. Baseline Version with 2011 attestation requirements.

(This Page Intentionally Blank)

TABLE OF CONTENTS

(This Page Intentionally Blank)

1 INTRODUCTION

1.1 PURPOSE

The purpose of the *CMS Annual Attestation Procedure* is to provide *CMS FISMA Controls Tracking System (CFACTS)* users with a systematic guide to completing the annual attestation process for FISMA systems and to provide the security personnel with CFACTS data entry responsibilities the necessary procedures for performing following in CFACTS:

- Documenting and testing system security for an applicable FISMA system.
- Updating applicable FISMA system information in CFACTS.
- Updating People and Inventory information in CFACTS.
- Completing and submitting Annual Attestation information in CFACTS.

1.2 BACKGROUND

As custodians of Citizen-based and other sensitive federal information, we all share the responsibility to protect sensitive information at CMS. Regular testing of information system security controls is the primary way that we can ensure that we are meeting this responsibility. In the Chief Information Officer (CIO) Directive 07-05 (the Directive) dated December 10 2007, the CIO defined the importance of conducting annual security controls testing for CMS systems to maintain on-going compliance with the Federal Information System Management Act (FISMA) of 2002 and the Federal Managers' Financial Integrity Act of 1982. The Directive and its attachments are available at http://www.cms.hhs.gov/InfoTechGenInfo/CIOD/list.asp as background material.

The process documented in this document provides the instructions for the FISMA security controls testing requirement, including documenting your attestation of the currency of your System Security Plan (SSP), Information Security Risk Assessment (IS RA), and the Contingency Plan (CP). This process requires action on the part of the business owners of FISMA-reported systems and applications. In order to support requirements from our FISMA auditors and the Department of Health and Human Services (HHS) Inspector General, CMS requires that the attestation be entered into the *CMS FISMA Controls Tracking System (CFACTS)* in accordance with the process described in Section 2 of this document, for the controls defined in Version 1.0, dated August 31, 2010, of the *CMS Information Security (IS) Acceptable Risk Safeguards (ARS) CMS Minimum Security Requirements (CMSR)*. It is expected that system/application developers/maintainers will assist in meeting these testing and reporting requirements. Business Owner completion of these FISMA requirements will be reported to HHS as part of the annual CMS FISMA compliance reporting.

For each of the FISMA-reported systems, CMS Business Owners are required to provide an attestation indicating that they have complied with the requirements for annual testing and the currency of the SSP, IS RA, and CP. This attestation shall be documented within the CFACTS.

Annual security control testing can be conducted by the Business Owners, the system developer/ maintainer, or by an independent entity. FISMA requires that all information system controls be *independently* tested at least once every three years. If independent security control testing is used for the annual security assessment requirement under FISMA, it may *also* count towards the triennial security control testing necessary for renewing an Authorization to Operate (ATO). For independent security assessments or audits, "independent" is defined in Section 1.4.1 of the *CMS Information Security Assessment Procedure*, which is available at http://www.cms.hhs.gov/informationsecurity/downloads/Assessment_Procedure.pdf. Note that the security control testing must have occurred after June 10 of the prior year to count towards the current year's annual security control testing requirements.

Attestations are due to be submitted no later than June 30 of each year (or the last workday prior; whichever is sooner.)

The attestation must include the security document date, and the date of the latest review (since June 10th of the prior year) of the following security documentation for each applicable system:

- System Security Plan (SSP)
- Information Security Risk Assessment (IS RA)
- Contingency Plan (CP). For the CP, the date of the latest CP test (since June 10 of the prior year) must also be updated.

If you have questions please contact the Office of the Chief Information Security Officer at mailto:ciso@cms.gov.

1.3 HOW TO USE THIS PROCEDURE

The *CMS Annual Attestation Procedure* is broken into two columns: *Procedure* and *Principle*. The *Procedure* column specifically addresses the necessary steps in order to complete the attestation process. The *Principle* column provides additional information about the procedure in order to fully understand why these steps are to be followed. Other documents are referenced in this column if more information is required.

1.4 OTHER RELEVANT PROCEDURES

Other relevant *Risk Management Handbook (RMH)* 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 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 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.

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 PROCEDURES

PROCEDURE	PRINCIPLE
2.1 ANNUAL ATTESTATION	
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 CONDITIONS	
1. Within the *Master Security Plan (MSP)*, the CMS Office of the Chief Information Security Officer (OCISO) has identified a set of *common* and *hybrid* controls for CMS systems. Use the MSP and the appropriate ARS CMSR security impact level to ascertain more information about each specific control requirement and to determine if the control provides the necessary protection for your system. If the system does not ***legitimately*** inherit these controls, then you are required to provide a compliance description for that portion of the control.	*For example, if your system does not reside in the Baltimore Data Center (BDC), then it would not be able to inherit those controls provided by the BDC.* *The Master Security Plan is available in the Information Security Library (http://www.cms.gov/informationsecurity/downloads/CMS_Master_Security_Plan.pdf).* *If control requirements are listed as hybrid controls in the MSP, your system is responsible for a portion of the control. You are required to provide a compliance description and test results for that portion of the control.*

PROCEDURE	PRINCIPLE
2. User has authorized access to the applicable CMS systems in CFACTS.	*Some user roles may not have the necessary access rights to enter vulnerabilities into CFACTS. Contact the OCISO 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.	

2.1.3 ANNUAL ATTESTATION PROCEDURE

2.1.3.1 DOCUMENTING AND TESTING SYSTEM SECURITY

1. Verify that all *Inheritable* controls are properly designated in CFACTS in accordance with RMH Volume II, Procedure 4.2, *Documenting Security Controls in CFACTS.*	*The process for designating* inherited *controls for a system is addressed in detail in the* Inheriting Security Controls *procedure.* *Also, ensure that all controls that are being* shared *(for inheritance by **other** systems) are properly designated in CFACTS using the* Sharing Inheritable Controls *procedure.*

PROCEDURE	PRINCIPLE
2. Determine which controls are to be tested to meet the *annual* security control assessment requirement for the system as follows:	*Security control* CA-2 *requires that security controls be assessed every 365 days (for all systems.) The applicable* Implementation Standards *detail how* many *controls a system must test annually. Each year, a different subset of controls must be tested so that ALL controls are tested during a 3-year period.*
a. Select any control families that have *not* been tested in the prior *two* annual assessments.	*Review the previous year(s) attestation(s) to ensure that same controls are not tested in the current year unless no other controls remain untested from the prior* ***two (2)*** *years. For Low and Moderate level systems, one third of the total set of control requirements* ***should*** *be tested each year, but all* ***must*** *be tested within a three-year period. For High-level systems—****No less than*** *one third* ***shall*** *be tested annually, and all* ***must*** *be tested within a three-year period. .*
b. ***ADD*** to the list of controls to be tested, *any* controls that had identified *Weaknesses* that have been *closed* since the applicable control was *last* tested.	*If a control requirement was previously identified as having an associated* Weakness, *and has been subsequently been changed to a status of* Pending Verification *or* Completed, *that control* ***must*** *be re-tested at the next available testing opportunity (usually the annual assessment) to verify the effectiveness of the remediation.*
c. ***ADD*** to the list of controls to be tested, *any* controls that had changes in the way the control has been implemented since the applicable control was *last* tested.	
d. ***ADD*** to the list of controls to be tested, *any* ***new*** controls *requirements* that have *never* been tested.	

PROCEDURE	PRINCIPLE
NOTE: ***ALL* individual security control implementation descriptions *MUST* be current in CFACTS—*not* just the controls to be tested this year.**	***All** security controls are required to have their compliance descriptions entered and maintained **current** in CFACTS, at all times. If **ANY** (not just the controls being tested this year) need to be **created** or **updated**, they **MUST** be created/updated prior to testing and finalizing the SSP.*
3. Update ***ALL*** security control compliance descriptions in accordance with RMH Volume II, Procedure 4.2, *Documenting Security Controls in CFACTS.*	*The process for properly documenting security controls in CFACTS is described in RMH Volume II, Procedure 4.2,* Documenting Security Controls in CFACTS.
4. Review the *Information Security Risk Assessment (IS RA)* by evaluating the following:	
a. Evaluate to determine if the *effectiveness* of security controls changed within the past year.	*Weaknesses that have been identified within the past year should be evaluated to determine if the overall risk to system operation is affected. These (resolved and unresolved) issues should be noted and evaluated in the* IS RA.
b. Evaluate to determine if the information system has undergone any *significant changes* to its *business objectives* or overall *mission importance* during within the past year.	*Changes to system operations, users populations, data handled, or logical processes can change the security state and the level of risk associated with continued operation of the system. These (resolved and unresolved) issues should be noted and evaluated in the* IS RA.
c. Evaluate to determine if the information system was subjected to any *significant changes* to its *security state* due to new or modified federal legislation, regulations, directives, policies, standards, or guidance.	*As security requirements change (based on changes to the threat environment), a system's security state can change dramatically, even though no changes were made to the system. These changes can change the level of risk associated with continued operation of the system. These (resolved and unresolved) issues should be noted and evaluated in the* IS RA.

PROCEDURE	PRINCIPLE
d. Evaluate to determine if the results from *ongoing monitoring* has identified new vulnerabilities that affect the overall risk to the system.	*As new vulnerabilities are identified and exploits that are more aggressive are developed, the system's level of overall risk can change dramatically, even though no changes were made to the system. These (resolved and unresolved) issues should be noted and evaluated in the* IS RA.
5. Update the *IS RA*, as required, to address the issues identified in Step 4	
6. Log into CFACTS using RMH Volume II, Procedure 1.1, *Accessing the CFACTS*.	
7. 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.*
8. From the *Identification* screen, click on the *SA&A Tracking* tab.	*Activates the* SA&A Tracking *screen.*
9. In the *Risk Assessment* section, perform the following:	
a. In the *RA Status* field, select *Completed* from the dropdown.	
b. In the *Last RA Date* field, enter the date that the last *IS RA* review was completed.	*This date **after** June 10 of the previous year.*
c. In the *Next RA Review Date* field, enter the date that the next *IS RA* review must be completed.	*Must be within the next 365 days from the* Last RA Date.
d. In the *RA Expiration Date* field, enter 365 days from the *Last RA Date*.	
e. In the *Next RA Date* field, enter 365 days from the *Last RA Date*.	

PROCEDURE	PRINCIPLE
10. Upload the updated *IS RA* to CFACTS as follows:	
NOTE: **The previous version of the *IS RA* should already be located in the *1 position.* If it is not there, load it before proceeding with the next step.**	*All systems with a current ATO are required to have ALL of security documentation loaded into CFACTS.*
a. In the *Risk Assessment* section, upload the new *IS RA* as follows:	
(1) Click on the *New* link.	*Opens the* Upload Support Document *screen.*
(2) In the *Title* field, type the *Date*, *Title*, and *Version* of the ***new*** *IS RA.*	*Example: "June 21 2012, IS RA XYZ System, Version 2.1"*
(3) Click on the *Browse* button and select the ***new*** *IS RA* document.	
(4) Click on the *Upload* button.	*Uploads the applicable IS RA document.*
(5) Click on the *Close* button.	*Returns to the* SA&A Tracking *screen.*
(6) Move the new *IS RA* to the *1* (topmost) position as follows:	
(a) In the *Risk Assessment* section, click on the *Move* link.	
(b) In the *From Artifact Position* field, select from the dropdown the document ***just uploaded*** in the steps above.	
(c) In the *To Artifact Position* field, select *1 – [Old document title]* from the dropdown.	
(d) Click on the *Save* button, then click on *OK* to confirm the move.	
(7) Click on the *Close* button.	*Returns to the* SA&A Tracking *screen.*

PROCEDURE	PRINCIPLE
11. Review the *System Security Plan (SSP)* by evaluating the following: a. Evaluate to determine if the description of the *Business Process(es)* that the system performs are accurate and current. b. Evaluate to determine if the description of the *system interconnections* is accurate and current. c. Evaluate the *Privacy Impact Assessment* to determine if the *PIA* for the information that the system *stores*, *processes*, or *transmits*, is accurate and current. d. Evaluate to determine if any other descriptions necessary to address *changes* to the system in the past year are accurate and current.	
12. Update the *SSP*, as required, to address the issues identified in Step 11.	
13. Log into CFACTS using RMH Volume II, Procedure 1.1, *Accessing the CFACTS*.	
14. 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.*
15. From the *Identification* screen, click on the *SA&A Tracking* tab.	*Activates the* SA&A Tracking *screen.*
16. In the *System Security Plan* section, perform the following: a. In the *SSP Status* field, select *Completed* from the dropdown. b. In the *SSP Target Completion Date* field, enter the *SA&A Expiration Date* from the *Security Assessment and Authorization* section.	

PROCEDURE	PRINCIPLE
c. In the *SSP Completion Date* field, enter the date that the *SSP* was last **revised**.	*This date should be reflected on the cover of the SSP loaded into CFACTS below.*
d. In the *SSP Reviewed this Year Date* field, enter the date that the SSP has been reviewed ***since June 10 of last year***.	*The SSP must be reviewed annual within each annual attestation period (since last June 10).*
e. In the *SSP Revision Date* field, enter the date that the *SSP* is scheduled for its ***next*** revision.	*This date should correspond with any future scheduled changes to the system.*
17. Upload the updated *SSP* to CFACTS as follows:	
NOTE: **The previous version of the *SSP* should already be located in the *1 position.* If it is not there, load it before proceeding with the next step.**	*All systems with a current ATO are required to have ALL of security documentation loaded into CFACTS.*
a. In the *System Security Plan* section, upload the new *SSP* as follows:	
(1) Click on the *New* link.	*Opens the* Upload Support Document *screen.*
(2) In the *Title* field, type the *Date*, *Title*, and *Version* of the ***new*** *SSP*.	*Example: "June 21 2012, SSP XYZ System, Version 2.1"*
(3) Click on the *Browse* button and select the ***new*** *IS RA* document.	
(4) Click on the *Upload* button.	*Uploads the applicable* SSP *document.*
(5) Click on the *Close* button.	*Returns to the* SA&A Tracking *screen.*
(6) Move the new *SSP* to the *1* (topmost) position as follows:	
(a) In the *System Security Plan* section, click on the *Move* link.	

PROCEDURE	PRINCIPLE
(b) In the *From Artifact Position* field, select from the dropdown the document ***just uploaded*** in the steps above.	
(c) In the *To Artifact Position* field, select *1 – [Old document title]* from the dropdown.	
(d) Click on the *Save* button, then click on *OK* to confirm the move.	
(e) Click on the *Close* button.	*Returns to the* SA&A Tracking *screen.*
18. Review the *Contingency Plan* and the *Annual Contingency Plan Test* as follows:	
a. Review the *Contingency Plan (CP)* by evaluating the following:	
(1) Evaluate to determine if the *Maximum Tolerable Disruption (MTD)* for the business have changed in the past year.	*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 have changed in the past year.	*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 have changed in the past year.	*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 have changed in the past year.	*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.*
b. Update the *CP*, as required, to address the issues identified from the evaluations performed in Step a.	
c. Test the updated *CP* as follows:	*Test in accordance with* CMS Information Security (IS) Application Contingency Plan (CP) Procedure *and applicable testing procedures and templates.*
(1) Develop an applicable *CP Test Plan*.	
(2) Test the *CP* in accordance with *CP Test Plan*.	
(3) Document the *CP* test in a *CP Test Report*.	
d. Update the *CP*, as necessary, to address deficiencies identified in the *CP* test, and documented in the *CP Test Report*.	
19. *Business Owner* certify *and* sign the *CP* and the *CP Test*.	*The* Business Owner *must sign the associated* Certification *page in the CP.*
20. Convert the signed *CP Certification* page to a PDF document to be loaded into CFACTS.	
21. Log into CFACTS using RMH Volume II, Procedure 1.1, *Accessing the CFACTS*.	
22. 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.*

PROCEDURE	PRINCIPLE
23. From the *Identification* screen, click on the *SA&A Tracking* tab.	*Activates the* SA&A Tracking *screen.*
24. In the *Contingency Plan* section, perform the following:	
a. In the *CP Status* field, select *Tested* from the dropdown.	
b. In the *CP Is Completed or Tested* field, maintain as populated by CFACTS.	*This field is automatically populated by CFACTS, and should say* Completed and tested *if the* CP Status *is* Tested.
c. In the *CP Initiation Date* field, enter the date that the last *CP* revision was started.	
d. In the *Last CP Completion Date* field, enter date that the *CP* was last ***revised*** (completed).	
e. In the *Next CP Review Date* field, enter the date that the CP was last *certified* as updated and tested.	*Must be recertified annually (since June 10 of last year.)*
f. In the *Next CP Revision Date* field, enter June 10 of next year.	
g. In the *Last CP Test Date* field, enter the date that the CP was last *tested*.	*Actual date that the CP was last tested.*
h. In the *Next CP Test Date* field, enter the date no-more-than 365 days after the *Last CP Test Date*.	

PROCEDURE	PRINCIPLE
25. Upload the updated *CP, CP Test* Report, and the *CP Certification* page to CFACTS as follows:	
NOTE: **The previous version of the *CP* should already be located in the *1 position,* the *CP Test Report* should be in the *2 position,* and the *CP Certification* page should be in the *100 position.* If any are not there, load the applicable document before proceeding with the next step.**	*All systems with a current ATO are required to have ALL of security documentation loaded into CFACTS.*
26. In the *Contingency Plan* section, upload the new *CP* and the *CP Test Report* as follows:	
a. For ***each*** of the *CP* and the *CP Test Report*, perform the following:	
(1) Click on the *New* link.	*Opens the* Upload Support Document *screen.*
(2) In the *Title* field, type the *Date, Title,* and *Version* of the ***new*** *CP* or *CP Test Report.*	*Example: "June 21 2012, CP XYZ System, Version 2.1"*
(3) Click on the *Browse* button and select the ***new*** *CP* or *CP Test Report* document.	
(4) Click on the *Upload* button.	*Uploads the applicable* CP *or* CP Test Report *document.*
(5) Click on the *Close* button.	*Returns to the* SA&A Tracking *screen.*
(6) Return to Step (1) and re-perform until each of the *CP, CP Test Report,* and *CP Certification* page are loaded.	

PROCEDURE	PRINCIPLE
b. Move the new *CP* to the *1* (topmost), the new *CP Test Report* to the *2* (second), and the *CP Certification* page to the *100* position, as follows:	
(1) In the *CP* section, click on the *Move* link.	
(2) In the *From Artifact Position* field, select from the dropdown the applicable document ***just uploaded*** in the steps above.	
(3) For the applicable document, perform ***one*** of the following steps:	
(a) For the *CP*: in the *To Artifact Position* field, select *1 – [Old CP title]* from the dropdown, ***or***	*Use this step for moving the current* CP.
(b) For the *CP Test Report*: in the *To Artifact Position* field, select *2 – [Old CP Test Report title]* from the dropdown, ***or***	*Use this step for moving the current* CP Test Report.
(c) For the *CP Certification Page*: in the *To Artifact Position* field, select *100 – [Old CP Certification Page title]* from the dropdown.	*Use this step for moving the current* CP Certification *page.*
(4) Click on the *Save* button, then click on *OK* to confirm the move.	
(5) Click on the *Close* button.	*Returns to the* SA&A Tracking *screen.*
(6) Return to Step (1) and re-perform until each of the *CP, CP Test Report,* and *CP Certification* page are in their correct positions.	- *Current* CP *should be in position 1,* - *Current* CP Test Report *should be in position 2,* - *Current* CP Certification *page should be in position 100.*

PROCEDURE	PRINCIPLE
27. In the *Privacy Impact Assessment* section, update, or verify, the *Privacy Impact Assessment (PIA)* as follows:	*Section 208 of the* E-Government Act of 2002 *requires all agencies to conduct PIAs for all new or substantially changed information systems that collect, maintain, or disseminate PII on the public*
a. Review the *Privacy Impact Assessment (PIA)* and evaluate to determine if the data associated with the system has been affected by any of the following factors:	*Any major change to the data that result in privacy risks shall be accurately reflected in the PIA.*
(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;*
(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*

PROCEDURE	PRINCIPLE
(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 any of the factors defined in Step a. 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 questions, contact the OCISO at mailto:ciso@cms.gov.*
c. For the *PIA Status* field, if the *PIA Status* is not *Completed*, perform the following:	*If an update is needed, the status cannot be* Completed.
(1) Update the *PIA* as necessary and route through the *CMS Privacy Office* for approval.	
(2) Upon *CMS Privacy Office* approval, update the *PIA Status* to *Completed.*	
d. For the *PIA Last Date* field, verify that the *PIA Last Date* reflects the latest *CMS Privacy Office* -approved *PIA*.	
e. For the *Next PIA Review Date* field, verify the *Next PIA Review Date* has not passed.	*HHS Policy (HHS OCIO IT 2009-0002.001) states, "Each PIA shall be reviewed and re-approved annually".*
f. For the *Next PIA Revision Date* field, verify the *Next PIA Revision Date* has not passed.	*For questions, contact the OCISO at mailto:ciso@cms.gov.*
g. Upload the latest *CMS Privacy Office* -approved *PIA* as follows:	
(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.*

PROCEDURE	PRINCIPLE
(3) From the *Identification* screen, click on the *SA&A Tracking* tab.	*Activates the* SA&A Tracking *screen.*
NOTE: **The previous version of the *PIA* should already be located in the *1 position.* If it is not there, load it before proceeding with the next step.**	*All systems with a current ATO are required to have ALL of security documentation loaded into CFACTS.*
(4) In the *PIA* section, upload the new *PIA* as follows:	
(a) Click on the *New* link.	*Opens the* Upload Support Document *screen.*
(b) In the *Title* field, type the *Date, Title,* and *Version* of the ***new*** *PIA.*	*Example: "June 21 2012, PIA XYZ System, Version 2.1"*
(c) Click on the *Browse* button and select the ***new*** *IS RA* document.	
(d) Click on the *Upload* button.	*Uploads the applicable PIA document.*
(e) Click on the *Close* button.	*Returns to the* SA&A Tracking *screen.*
(f) Move the new *PIA* to the *1* (topmost) position as follows:	
i. In the *Privacy Impact Assessment* section, click on the *Move* link.	
ii. In the *From Artifact Position* field, select from the dropdown the document ***just uploaded*** in the steps above.	
iii. In the *To Artifact Position* field, select *1 – [Old document title]* from the dropdown.	
iv. Click on the *Save* button, then click on *OK* to confirm the move.	
v. Click on the *Close* button.	*Returns to the* SA&A Tracking *screen.*

PROCEDURE	PRINCIPLE
28. In the *System of Records Notice* section, perform ***one*** of the following:	
a. If the *PIA* indicates that **no** *Privacy Act* information is applicable for this system, perform the following:	*Perform this step if there **is no*** Privacy Act *information associated with this system.*
(1) For the *SORN Status* field, select *Not Applicable* from the dropdown list.	
(2) For the *SORN Published Date* field, enter *TBD*.	
(3) For the *SORN ID* field, leave blank.	
(4) For the *Next SORN Review Date* field, enter *TBD*.	
(5) For the *Next SORN Revision Date* field, enter *TBD*.	
b. If the *PIA* indicates that there **is** *Privacy Act* information is applicable for this system, perform the following:	*Perform this step if there **is*** Privacy Act *information associated with this system.*
(1) For the *SORN Status* field, verify/update the *SORN Status*. If the *SORN Status* is not *Completed*, perform the following:	
(a) ***IMMEDIATELY*** coordinate with the *CMS Privacy Office* to complete the SORN.	*Systems operating with* Privacy Act *information, without an applicable SORN, are operating in violation of the* Privacy Act of 1974.
(b) Upon *CMS Privacy Office* direction, update the *SORN Status* to *Completed.*	
(2) For the *SORN Published Date* field, verify that the *SORN Published Date* reflects the latest approved *SORN*.	*SORNs are updated periodically to reflect updates usage cases for the collected* Privacy Act *information*
(3) For the *SORN ID* field, enter ALL of the applicable *SORN IDs*.	*Some systems may reference several SORNs.*

PROCEDURE	PRINCIPLE
(4) For the *Next SORN Review Date* field, verify the *Next SORN Review Date* has not passed.	*For questions, contact the OCISO at mailto:ciso@cms.gov.*
(5) For the *Next SORN Revision Date* field, verify the *Next SORN Revision Date* has not passed.	*For questions, contact the OCISO at mailto:ciso@cms.gov.*
(6) Upload the latest *CMS Privacy Office* -approved *SORNs* as follows:	*Active and current CMS* System of Records Notices *can be found at https://www.cms.gov/PrivacyActSystemofRecords/SR/list.asp*
(a) Log into CFACTS using RMH Volume II, Procedure 1.1, *Accessing the CFACTS.*	
(b) 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.*
(c) From the *Identification* screen, click on the *SA&A Tracking* tab.	*Activates the* SA&A Tracking *screen.*
NOTE: **The previous version of the *PIA* should already be located in the *1 position.* If it is not there, load it before proceeding with the next step.**	*All systems with a current ATO are required to have ALL of security documentation loaded into CFACTS.*
(d) In the *System of Records Notice* section, upload new *SORNs* as follows:	*Load all of the latest SORNs as a single zipped file.*
(e) Click on the *New* link.	*Opens the* Upload Support Document *screen.*
(f) In the *Title* field, type the *Date, Title,* and *Version* of the ***new*** *SORNs*.	*Example: "June 21 2012, SORNs XYZ System, Version 2.1"*
(g) Click on the *Browse* button and select the ***new*** *SORN* file.	
(h) Click on the *Upload* button.	*Uploads the applicable PIA document.*

PROCEDURE	PRINCIPLE
(i) Click on the *Close* button.	*Returns to the* SA&A Tracking *screen.*
(j) Move the new *SORNs* to the *1* (topmost) position as follows:	
i. In the *System of Records Notice* section, click on the *Move* link.	
ii. In the *From Artifact Position* field, select from the dropdown the document ***just uploaded*** in the steps above.	
iii. In the *To Artifact Position* field, select *1 – [Old document title]* from the dropdown.	
iv. Click on the *Save* button, then click on *OK* to confirm the move.	
v. Click on the *Close* button.	*Returns to the* SA&A Tracking *screen.*
29. In the *Miscellaneous* section, perform the following:	
a. In the *System Categorization Date* field, enter the date that the *system's security category* was ***last*** evaluated/re-evaluated.	*Security category should be evaluated periododically when the system is updated to ensure that system changes are not changing the security category.*
NOTE: **A *Security Integrated into the Lifecycle* field value of *Not Applicable* is not allowed at CMS.**	*Systems have either integrated security into the lifecycle or not—but it is always applicable.*
b. In the *Security Integrated into the Lifecycle* field, select either *Yes* or *No*, as appropriate, from the dropdown list.	*This field indicates whether security control requirements are included as system (non-functional) design requirements, and were integrated in **all** phases of the system development lifecycle for this system during the development or last significant modification.*

PROCEDURE	PRINCIPLE
c. If the *Security Integrated into the Lifecycle* field value is *Yes*, perform the following:	
(1) For ***each*** of the *System Design Document (SDD)* and the *Interface Control Document (ICD)*, upload the ***most current*** version(s) as follows:	*The SDD and ICD documents will assist security personnel to determine the security boundaries of the system. When developing the system, or system changes, security considerations should be addressed in the design documents.*
(a) Click on the *New* link.	*Opens the* Upload Support Document *screen.*
(b) In the *Document Type* field, select *Other* from the dropdown list.	
(c) In the *Title* field, type the *Date, Title,* and *Version* of the ***new*** *SDD* or *ICD.*	*Example: "June 21 2012, ICD XYZ System, Version 2.1"*
(d) Click on the *Browse* button and select the ***new*** *SDD* or *ICD* document.	
(e) Click on the *Upload* button.	*Uploads the applicable* SDD *or* ICD *document.*
(f) Click on the *Close* button.	*Returns to the* SA&A Tracking *screen.*
(g) Return to Step 26.a. (1) and re-perform until all of the *SDD* and *ICD* documents is loaded.	
(2) Move the new *SDD* to the *100* position and the *ICD* to the *101* position, as follows:	*The most current document version should be at the top of the list.*
(a) In the *Miscellaneous* section, click on the *Move* link.	
(b) In the *From Artifact Position* field, select from the dropdown the applicable document ***just uploaded*** in the steps above.	

PROCEDURE	PRINCIPLE
(c) For the applicable document, perform ***one*** of the following steps:	
i. For the *SDD*: in the *To Artifact Position* field, select *1 – [Old SDD title]* from the dropdown, ***or***	*Use this step for moving the current* SDD.
ii. For the *ICD*: in the *To Artifact Position* field, select *2 – [Old ICD title]* from the dropdown.	*Use this step for moving the current* ICD.
(d) Click on the *Save* button, then click on *OK* to confirm the move.	
(e) Click on the *Close* button.	*Returns to the* SA&A Tracking *screen.*
(f) Return to Step (2) and re-perform until each of the *SDD*, and *ICD* are in their correct positions.	- *Current* SDD *should be in position 100,* - *Current* ICD *should be in position 101.*
30. Test ***EACH*** of the control requirements (including all *Implementation Standards* and *Enhancements*) selected in Step 2, in accordance with ARS control requirement CA-2 and CMS security assessment procedures.	*For each security control assessment failure, be sure to develop and appropriate weakness and corrective action plan.*
31. For the ***EACH*** of the controls tested, document or update the applicable security control *assessment* information in accordance with RMH Volume II, Procedure 5.6, *Documenting Security Control Effectiveness in CFACTS.*	*The results of testing for **EACH** control requirement (including all* Implementation Standards *and* Enhancements*) must be documented in CFACTS—even (especially) results for testing controls that have* passed.

2.1.3.2 UPDATING SYSTEM INFORMATION IN CFACTS.

1. Log into CFACTS using RMH Volume II, Procedure 1.1, *Accessing the CFACTS.*	

PROCEDURE	PRINCIPLE
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. Select, or verify selected, the *General Information* radio button.	*Displays the* General Information *view of the* Identification *screen.*
4. 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**. *For questions, contact the OCISO at mailto:ciso@cms.gov.*
b. Select, or verify selected, ***Yes*** for ***all*** others.	
5. For the *Program* field, leave as *Not Applicable* unless specifically directed by OCISO.	*For questions, contact the OCISO at mailto:ciso@cms.gov.*
6. For the *Site* field, leave as *Not Applicable* unless specifically directed by OCISO.	*For questions, contact the OCISO at mailto:ciso@cms.gov.*
7. For the *Parent System* field, leave as *Not Applicable* unless specifically directed by OCISO.	*For questions, contact the OCISO at mailto:ciso@cms.gov.*
8. For the *Acronym* field, leave as currently populated unless specifically directed by OCISO.	*This field is matched with enterprise architecture data maintained at HHS, and cannot be changed without coordination with HHS. For questions, contact the OCISO at mailto:ciso@cms.gov.*
9. For the *Number of Users* field, enter the approximate number of users for this system.	
10. For the *System Type* field, select the appropriate *System Type* from the dropdown.	
11. For the *This System is an Operational Network* field, leave as *No* unless specifically directed by OCISO.	*For questions, contact the OCISO at mailto:ciso@cms.gov.*

PROCEDURE	PRINCIPLE
12. For the *Financial System* field, leave as currently populated unless specifically directed by OCISO.	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. For questions, contact the OCISO at mailto:ciso@cms.gov.*
13. For the *Is Critical Asset* field, leave as *No* unless specifically directed by OCISO.	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. For questions, contact the OCISO at mailto:ciso@cms.gov.*
14. For the *SDLC Status* field, select, or verify selected, the appropriate *SDLC Status,* from the dropdown list.	*Only* **Operational** *systems are required to perform annual assessment. If you selected any* other *SDLC status, contact the OCISO at mailto:ciso@cms.gov.*
15. For the *Creation Date* field, leave as populated by CFACTS.	
16. Click on the *Save* button.	
17. On the *System Identification* tab, select the *Detailed Description* radio button.	*Displays the* Detailed Description *view of the* System Identification *screen.*
18. 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.*
19. For the *Prepared By* field, enter the name of the POC responsible for performing this procedure.	
20. For the *Purpose* field, describe the business objectives and purpose of this system.	

PROCEDURE	PRINCIPLE
2.1.3.3 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.	
4. Select the *POCs* radio button.	*Displays the* POCs *view of the* People and Inventory *screen.*
5. Verify that a POC entry exists for: *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 the OCISO.*
6. If any of the POC entries listed above are missing, perform the following for each missing POC:	*A system must have at least a Business Owner, System Developer/Maintainer, and Information System Security Officer (ISSO).*
a. Click on the *New* link.	*Opens the* Add Information Point of Contact *screen.*
b. In the *Name* field, enter the full *Name* of the applicable POC.	
c. In the *SA&A Role* field, select the applicable *SA&A Role* of the applicable POC from the dropdown list.	
d. In the *HR Title* field, enter the applicable *HR Title* of the applicable POC.	

PROCEDURE	PRINCIPLE
e. In the *Component* field, enter the CMS business *Component* of the applicable POC.	*For contractors, enter the* Company *name.*
f. In the *Address* field, enter the full mailing *Address* of the applicable POC.	*For CMS employees, include any applicable* Mail Stop.
g. In the *Phone* field, enter the business *Phone* number of the applicable POC.	
h. In the *Email* field, enter the full *Email* address of the applicable POC.	
i. 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.	
j. In the *Fax* field, enter the *Fax* number of the applicable POC.	
k. In the *Responsibility* field, describe the SA&A *Responsibilities* of the applicable POC.	
l. Click on the *Save* Button.	*Save information and returns to the* People and Inventory *screen.*
m. Perform one of the following:	
(1) To add additional POCs, return to step a. ***or***	*For contractors, add applicable contractor security personnel (such as SSO) and other applicable CFACTS data-entry and security personnel.*
(2) To continue, proceed to Step 7.	
7. Add or update system *interconnections* in accordance with the *Document System Interconnections* procedure in RMH Volume II, Procedure 4.2, *Documenting Security Controls in CFACTS*.	

PROCEDURE	PRINCIPLE
2.1.3.4 COMPLETING ANNUAL ATTESTATION DOCUMENTATION	
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. From the *Identification* screen, click on the *SA&A Tracking* tab.	*Activates the* SA&A Tracking *screen.*
4. In the *Annual Assessment* section, perform the following:	
a. In the *Annual Assessment Status* field, select *Completed* from the dropdown.	
b. In the *Start Date* field, enter the *Start Date* of the Annual Assessment.	
c. In the *Estimated End Date* field, enter the date that the Annual Assessment was completed.	
d. In the *Last Assessment Date* field, enter the date that the Annual Assessment was completed.	
e. In the *Next Annual Assessment Date* field, enter **no later than** June 10 of next year.	
f. Click on the *Save* button.	*Saves data entered on this screen.*
5. Complete the *CMS Annual Attestation Memorandum* as follows:	*The memorandum template is available in the H: Drive under CISO Forum Slides folder.*
a. *Business Owner* of the system signs the *Memorandum.*	

PROCEDURE	PRINCIPLE
b. Convert the signed *Memorandum* to a PDF file.	
6. In the *Annual Assessment* section, perform the following:	
NOTE:	
The previous version of the *Annual Attestation Memorandum* should already be located in the *100 position*. If it is not there, load it before proceeding with the next step.	*All systems with a current ATO are required to have ALL of security documentation loaded into CFACTS.*
a. In the *Annual Assessment* section, upload the new *Annual Attestation Memorandum* as follows:	
(1) Click on the *New* link.	*Opens the* Upload Support Document *screen.*
(2) In the *Title* field, type the *Date* and *Title* of the ***new*** *Annual Attestation Memorandum.*	*Example: "June 21 2012, XYZ System Annual Attestation Memorandum"*
(3) Click on the *Browse* button and select the ***new*** *IS RA* document.	
(4) Click on the *Upload* button.	*Uploads the applicable* Annual Attestation Memorandum *document.*
(5) Click on the *Close* button.	*Returns to the* SA&A Tracking *screen.*
(6) Move the new *Annual Attestation Memorandum* to the *100* (topmost) position as follows:	
(a) In the *Annual Assessment* section, click on the *Move* link.	
(b) In the *From Artifact Position* field, select from the dropdown the document ***just uploaded*** in the steps above.	

PROCEDURE	PRINCIPLE
(c) In the *To Artifact Position* field, select *100 – [Old document title]* from the dropdown.	
(d) Click on the *Save* button, then click on *OK* to confirm the move.	
(e) Click on the *Close* button.	*Returns to the* SA&A Tracking *screen.*
7. On the *SA&A Tracking* screen, click the Save button.	*Saves all data entered.*

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 15:45:51 -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.