CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES
OFFICE OF INFORMATION SERVICES

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

ESIG
Enterprise Information
Security Group
Risk Management, Oversight,
And Monitoring

Risk Management Handbook
Volume II
Procedure 7.3
CMS Annual Attestation Procedure

FINAL
Version 1.3
February 3, 2014

Document Number: CMS-CISO-2014-vII-pr7.3

(This Page Intentionally Blank)

SUMMARY OF CHANGES IN *CMS ANNUAL ATTESTATION PROCEDURE* VERSION 1.3, DATED FEBRUARY 3, 2014

1. Updated to address changes to attestation process changes for 2014.

SUMMARY OF CHANGES IN *CMS ANNUAL ATTESTATION PROCEDURE* VERSION 1.2, DATED JANUARY 25, 2013

1. Updated to address changes to attestation process changes for 2013.

SUMMARY OF CHANGES IN *CMS ANNUAL ATTESTATION PROCEDURE* VERSION 1.1, DATED FEBRUARY 13, 2012

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

SUMMARY OF CHANGES IN *CMS ANNUAL ATTESTATION PROCEDURE* VERSION 1.0, DATED JANUARY 19, 2011

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 the 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. A critical factor for maintaining on-going compliance with Federal Information System Management Act (FISMA) of 2002, and the Federal Managers' Financial Integrity Act (FMFIA) of 1982, is for Business Owners, in coordination with appropriate security personnel, to annually test their internal controls and dedicate sufficient resources to accomplish this test. These resources include budget (if external resources are to be used to support the testing), and person hours (if internal personnel are to be engaged in this activity). They are required to schedule and perform the test; and oversee the development and completion of corrective action plans for vulnerabilities noted during the testing.

The annual requirement has been interpreted by the *Office of Management and Budget (OMB)* as being within 365 calendar days of the prior test. Over a three-year period all controls applicable to the system or application, as set forth in the *CMS Information Security (IS) Acceptable Risk Safeguards (ARS) CMS Minimum Security Requirements (CMSR)* (as amended), must be tested. It is the responsibility of Business Owners, in coordination with developer/maintainers of CMS applications and systems, to meet this requirement.

The CMS promulgates and operationalizes this requirement within this procedure, and reiterates the importance of conducting annual security controls testing for CMS systems to maintain on-going compliance with FISMA and FMFIA.

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 this document, for the controls defined in Version 2.0, dated September 20, 2013, 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.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html. 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.

Additionally, the Office of Acquisition and Grants Management (OAGM) memorandum New CMS Information Security Requirements dated April 12, 2013 requires an annual contractor attestation. For this attestation, refer to the OAGM memorandum and enclosure (2) template for this annual submission.

Personnel completing the Annual Attestation should have intimate knowledge of system security operations as well as how to work within CFACTS. CFACTS users should understand the limitations of the application such as; session time outs, saving any changes or updates prior to closing windows, and navigation methods throughout the CFACTS environment.

If you have questions please contact the Enterprise Information Security Group (EISG) at mailto:ciso@cms.hhs.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 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 explains how 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 provides a systematic guide to review and ensure the accuracy and completeness of security related information for systems in CFACTS.
- RMH Volume II, Procedure 7.8, *Key Updates*. This procedure explains how to ensure that Weaknesses are properly documented and managed in CFACTS. This procedure is required to ensure that all information in CFACTS is updated to reflect recent events.

Other relevant procedures that are not yet incorporated into the *Risk Management Handbook* include:

- *CMS System Security Plan (SSP) Procedure*.
- *CMS Information Security Risk Assessment (IS RA) Procedure*.
- *CMS Information Security (IS) Contingency Plan (CP) Procedures*.

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

2 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. Use 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*** FULLY inherit these controls, then you are required to provide a compliance description for that portion of the control for which the local system must perform.

Example: *If* a *system does not reside in the Baltimore Data Center (BDC), then it will not be able to inherit those controls provided by the BDC.*

Fully-*inheritable control effectiveness cannot be influenced by individual systems. If an individual (inheriting) system is capable of influencing the effectiveness of an inheritable control, then that control cannot be considered to be FULLY-inheritable—which mandates that additional documentation and testing be required at the system-specific level to ensure that the control is implemented at its full effectiveness.*

Example*: If an inherited control requires that the inheriting system be configured to utilize* Active Directory *as an access control method, explain how this was configured and is managed during the life-cycle.*

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 EISG at mailto:ciso@cms.hhs.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 REVIEW AND UPDATE SYSTEM INFORMATION IN CFACTS

1. Perform necessary updates of the system documentation in accordance with RMH Volume II, Procedure 7.8, *Key Updates*.

This procedure explains how to ensure that Weaknesses are properly documented and managed in CFACTS. This procedure is required to ensure that all information in CFACTS is updated to reflect any events that may have occurred since the last review.

2. Verify the system information documented in CFACTS and update as necessary in accordance with RMH Volume II, Procedure 2.6, *Information System Description* using the *Creating or Updating System Information in CFACTS procedure.*

This procedure is used to create or update system information in CFACTS.

3. Perform a review of the system security information in accordance with RMH Volume II, Procedure 6.3, *Security Information Review*.

This procedure provides a systematic guide to review and ensure the accuracy and completeness of security related information for systems in CFACTS.

PROCEDURE | **PRINCIPLE**

2.1.3.2 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.*

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 the 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 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.*

PROCEDURE	**PRINCIPLE**
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.	
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.

PROCEDURE	PRINCIPLE
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.
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 *Security Authorization* tab.	*Activates the* Security Authorization *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. This date will be available in the Review Log of the current IS RA (if a current FISMA system) or the date on the title page (if a new FISMA system).*

PROCEDURE	PRINCIPLE
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*.	
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 (topmost) 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:	
CAUTION: **Do *NOT* use the *Upload* link. Using the *Upload* link will overwrite (destroy) the previous document version in the CFACTS repository.**	
(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 20xx, 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* Security Authorization *screen.*

PROCEDURE	**PRINCIPLE**
(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 or next (topmost) – [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* Security Authorization *screen.*
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.	*This is a system/business process, not a contract description.*
b. Evaluate to determine if the description of the *system interconnections* is accurate and current.	
c. 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.*

PROCEDURE	PRINCIPLE
15. From the *Identification* screen, click on the *Security Authorization* tab.	*Activates the* Security Authorization *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 *Security Authorization Expiration Date* from the *Security Authorization* section.	
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). This date is available in the Review Log of the current SSP.*
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.*

PROCEDURE	**PRINCIPLE**
17. Upload the updated *SSP* to CFACTS as follows:	
NOTE: **The previous version of the *SSP* should already be located in the *1 (topmost) 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:	
CAUTION: **Do *NOT* use the *Upload* link. Using the *Upload* link will overwrite (destroy) the previous document version in the CFACTS repository.**	
(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 20xx, SSP XYZ System, Version 2.1"*
(3) Click on the *Browse* button and select the ***new*** *SSP* document.	
(4) Click on the *Upload* button.	*Uploads the applicable* SSP *document.*
(5) Click on the *Close* button.	*Returns to the* Security Authorization *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.	
(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 *1 (topmost) – [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* Security Authorization *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 has 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 has 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 has 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 has 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 *name/signature* ***must*** *match the name of the Business Owner listed in CFACTS. He/she 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*.	

PROCEDURE	PRINCIPLE
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.*
23. From the *Identification* screen, click on the *Security Authorization* tab.	*Activates the* Security Authorization *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).	*This date is available in the Review Log of the current CP (if a current FISMA system) or the date on the title page (if a new FISMA system).*
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 (topmost) position,* the *CP Test Report* should be in the *2 or next (topmost) position,* and the *CP Certification* page should be in the *100 or next (topmost) 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*, the *CP Test Report*, and the *CP Certification* page as follows:	
a. For ***each*** of the *CP*, the *CP Test Report*, and the *CP Certification* page perform the following:	
CAUTION: **Do *NOT* use the *Upload* link. Using the *Upload* link will overwrite (destroy) the previous document version in the CFACTS repository.**	
(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 20xx, 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* Security Authorization *screen.*

PROCEDURE	PRINCIPLE
(6) Return to Step (1) and re-perform until each of the *CP*, *CP Test Report*, and *CP Certification* page are loaded.	
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 or next (topmost)* 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 or next (topmost)– [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 or next (topmost) – [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 or next (topmost) – [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* Security Authorization *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. 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:	*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.* *Any major change to the data that result in privacy risks shall be accurately reflected in the PIA.*
a. Conversions of *form.*	*A conversion from paper-based methods to electronic systems.*
b. *Anonymous to non-anonymous*.	*The system's function, as applied to an existing information collection, changes anonymous information into PII;*
c. 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;*
d. 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;*
e. 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;*
f. *Commercial* sources.	*PII, obtained from commercial or public sources, is systematically integrated into the existing information system's database;*
g. New *interagency* uses.	*When agencies work together on shared functions involving significant new uses or exchanges of PII;*
h. 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
i. 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.*
28. If any of the factors defined in Step 27. has occurred, immediately contact the *CMS Privacy Office at* mailto:pia@cms.hhs.gov 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 EISG at mailto:ciso@cms.hhs.gov and the Privacy Team at mailto:pia@cms.hhs.gov*.
29. Provide the HHS published *PIA* for the system.	*Upon completion of each assessment, agencies are required to make* PIA*s publicly available. This information is available on the HHS.gov website.* *Because the current fiscal year* PIA *list is not available at the time of the attestation, systems must provide the previous year's information. The HHS* PIA *may not be available for new systems.*
a. From a browser, enter the HHS PIA URL: *http://www.hhs.gov/pia/*.	
b. Select the *Centers for Medicare & Medicaid Services Privacy Impact Assessments* link.	
c. Search for the system's *PIA*.	
d. Take a screenshot of the system's *PIA*.	
e. If the *PIA* is not available on the website, contact the *CMS Privacy Office at* mailto:pia@cms.hhs.gov.	
30. Log into CFACTS using RMH Volume II, Procedure 1.1, *Accessing the CFACTS*.	
31. 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**
32. From the *Identification* screen, click on the *Security Authorization* tab.	*Activates the* Security Authorization *screen.*
33. In the *Privacy Impact Assessment* section, perform the following:	
a. 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.*	
b. For the *Last PIA Date* field, verify that the *Last PIA Date* reflects the latest *CMS Privacy Office* -approved *PIA*.	
c. 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."*
d. For the *Next PIA Revision Date* field, verify the *Next PIA Revision Date* has not passed.	*For questions, contact the EISG at mailto:ciso@cms.hhs.gov and the Privacy Team at mailto:pia@cms.hhs.gov.*
34. Upload the latest *CMS Privacy Office* -approved *PIA* and HHS *PIA* screenshot as follows:	
NOTE: **The previous version of the *PIA* should already be located in the *1 or next (topmost) position,* and the HHS *PIA* screenshot should be in the *100 or next (topmost) 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 the security documentation loaded into CFACTS.*
35. In the *PIA* section, upload the new *PIA* and HHS *PIA* screenshot as follows:	

PROCEDURE	**PRINCIPLE**
a. For ***each*** of the *PIA* and HHS *PIA* screenshot, perform the following:	
CAUTION: **Do *NOT* use the *Upload* link. Using the *Upload* link will overwrite (destroy) the previous document version in the CFACTS repository.**	
(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*** *PIA or HHS PIA screenshot.*	*Example: "June 21 20xx, PIA XYZ System, Version 2.1"*
(3) Click on the *Browse* button and select the ***new*** *PIA* or HHS PIA screenshot document.	
(a) Click on the *Upload* button.	*Uploads the applicable PIA document.*
(b) Click on the *Close* button.	*Returns to the* Security Authorization *screen.*
(4) Return to Step (1) and re-perform until each of the *PIA* and HHS *PIA* screenshot are loaded.	
b. Move the new *PIA* to the *1* (topmost) and the HHS *PIA* screenshot to the *100 or next (topmost)* position as follows:	
(1) In the *Privacy Impact Assessment* section, click on the *Move* link.	
(2) In the *From Artifact Position* field, select from the dropdown the document ***just uploaded*** in the steps above.	

PROCEDURE	**PRINCIPLE**
(3) For the applicable document, perform ***one*** of the following steps:	
(a) For the PIA: in the *To Artifact Position* field, select *1 or next (topmost) – [Old PIA title]* from the dropdown.	*Use this step for moving the current* PIA.
(b) For the HHS PIA screenshot: in the *To Artifact Position* field, select *100 or next (topmost) – [Old* HHS *PIA* screenshot *title]* from the dropdown.	*Use this step for moving the current HHS* PIA *screenshot.*
(4) Click on the *Save* button, then click on *OK* to confirm the move.	
(5) Click on the *Close* button.	*Returns to the* Security Authorization *screen.*
(6) Return to Step (1) and re-perform until each of the *PIA* and HHS *PIA* screenshot are in their correct positions.	-*Current* PIA *should be in position 1,* -*Current HHS* PIA *screenshot should be in position 100.*
36. 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*.	

PROCEDURE	**PRINCIPLE**
b. If the *PIA* indicates that there **is** *Privacy Act* information 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 updated 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.*
(4) For the *Next SORN Review Date* field, verify the *Next SORN Review Date* has not passed.	*For questions, contact the EISG at mailto:ciso@cms.hhs.gov and the Privacy Team at mailto:pia@cms.hhs.gov.*
(5) For the *Next SORN Revision Date* field, verify the *Next SORN Revision Date* has not passed.	*For questions, contact the EISG at mailto:ciso@cms.hhs.gov and the Privacy Team at mailto:pia@cms.hhs.gov.*
(6) Upload the latest *CMS Privacy Office* -approved *SORNs* as follows:	*Active and current CMS* System of Records Notices *can be found at http://www.cms.gov/Regulations-and-Guidance/Guidance/PrivacyActSystemofRecords/Systems-of-Records.html.*
(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.*

PROCEDURE	**PRINCIPLE**
(c) From the *Identification* screen, click on the *Security Authorization* tab.	*Activates the* Security Authorization *screen.*
NOTE:	
The previous version of the *SORN* should already be located in the *1 or next (topmost) 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.*
CAUTION:	
Do *NOT* use the *Upload* link. Using the *Upload* link will overwrite (destroy) the previous document version in the CFACTS repository.	
(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 20xx, 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 SORN document.*
(i) Click on the *Close* button.	*Returns to the* Security Authorization *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.	

PROCEDURE	PRINCIPLE
iii. In the *To Artifact Position* field, select *1 or next (topmost) – [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* Security Authorization *screen.*
37. 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 periodically when the system is updated to ensure that system changes are not changing the security category.*
NOTE: **A *Security Integrated into 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 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 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.*
CAUTION: **Do *NOT* use the *Upload* link. Using the *Upload* link will overwrite (destroy) the previous document version in the CFACTS repository.**	
(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 20xx, 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* Security Authorization *screen.*
(g) Return to Step 26.a. (1) and re-perform until all of the *SDD* and *ICD* documents are loaded.	
(2) Move the new *SDD* to the *100 or next (topmost)* position and the *ICD* to the *101 or next (topmost)* 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.	

PROCEDURE	PRINCIPLE
(b) In the *From Artifact Position* field, select from the dropdown the applicable document ***just uploaded*** in the steps above.	
(c) For the applicable document, perform ***one*** of the following steps:	
i. For the *SDD*: in the *To Artifact Position* field, select *100 or next (topmost)– [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 101 *or next (topmost) – [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* Security Authorization *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.*
38. 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 an appropriate weakness and corrective action plan.*
39. 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.

PROCEDURE	PRINCIPLE
2.1.3.3 COMPLETING ANNUAL ATTESTATION DOCUMENTATION	*Attestations are due to be submitted no later than June 30 of each year (or the last workday prior; whichever is sooner).*
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 *Security Authorization* tab.	*Activates the* Security Authorization *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.	*This would be the same date as the* Annual Attestation Memorandum.
d. In the *Last Annual Assessment Date* field, enter the date that the Annual Assessment was completed.	*This would be the same date as the* Annual Attestation Memorandum.
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.*

PROCEDURE	PRINCIPLE
5. Complete the *CMS Annual Attestation Memorandum* as follows:	*The memorandum template is available in the H: Drive under CISO Forum Slides folder. It is also available in Appendix A of this document.*
a. For each system, enter the System Acronym and required dates.	
(1) In the *System Acronym* field, enter the System Acronym as listed in CFACTS.	
(2) In the *POC List Review* field, enter the date the system POCs were reviewed.	*Formal testing is not required for the* POC List Review.
(3) In the *SSP Update* field, enter the date from the CFACTS *SSP Reviewed this Year Date* field.	
(4) In the *IS RA Update* field, enter the date from the CFACTS *LAST RA Date* field.	
(5) In the *CP Update* field, enter the date from the CFACTS *Last CP Completion Date* field.	
(6) In the *CP Test* field, enter the date from the CFACTS *Last CP Test Date* field.	
(7) In the *1/3 Controls Test* field, enter the date from the CFACTS *Last SCA Date* field.	
b. In the *Carbon Copy (cc)* section, enter the names of the CMS System Developer/ Maintainer and the Information System Security Officer (ISSO) and identify each with the appropriate title (Developer/Maintainer or Information System Security Officer).	
c. *Business Owner* of the system signs the *Memorandum.*	
d. Convert the signed *Memorandum* to a PDF file.	

PROCEDURE	PRINCIPLE
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 or next (topmost) 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:	
CAUTION: **Do *NOT* use the *Upload* link. Using the *Upload* link will overwrite (destroy) the previous document version in the CFACTS repository.**	
(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 20xx, XYZ System Annual Attestation Memorandum"*
(3) Click on the *Browse* button and select the ***new*** *Annual Attestation Memorandum* document.	
(4) Click on the *Upload* button.	*Uploads the applicable* Annual Attestation Memorandum *document.*
(5) Click on the *Close* button.	*Returns to the* Security Authorization *screen.*
(6) Move the new *Annual Attestation Memorandum* to the *100* (*or next (topmost)*) position as follows:	
(a) In the *Annual Assessment* 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 *100 or next (topmost) – [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 Security Authorization *screen.*

7. On the *Security Authorization* screen, click the Save button.

Saves all data entered.

8. Provide the hard copy of the *Annual Attestation Memorandum* to EISG.

If using interoffice mail, the location is: Central Office, Mailstop N1-24-08.

2.2 ATTESTATION REVIEW

2.2.1 PROCEDURE USERS

1. EISG Reviewer.

2. EISG Quality Assurance (QA).

3. EISG federal employee.

4. POA&M federal employee.

5. POA&M team member.

2.2.2 INITIAL CONDITIONS

1. The hard copy of the *Annual Attestation Memorandum* was provided to EISG, and the (signed) soft copy of the memorandum is in CFACTS.

PROCEDURE	PRINCIPLE
2. All templates and spreadsheets are available on the EISG organizational share drive for the EISG reviewer.	*Examples include the* Attestation folder, Attestation Review Checklist, Attestation Tracking Spreadsheet, Action Required Email Template, Pass/Fail E-mail templates, *and* POA&M templates.

2.2.3 ATTESTATION REVIEW PROCEDURE

2.2.3.1 INITIAL QUICK CHECK

1. If the *Initial* Conditions are not met and the *Annual Attestation Memorandum* for a system is not received by EISG by the designated completion date, notify the system *Business Owner*.	*If the* CMS Annual Attestation Procedure *is not followed, the* Action Required Email Template *will be completed and sent to the system* Business Owner. *The template is an internal document for the use of EISG and is available on the EISG organizational share drive.*
a. Either *EISG QA* or the *EISG federal employee* completes the *ACTION REQUIRED FY## Attestation* email template and sends it to the *Business Owner*.	*If there are multiple systems without attestations with the same Business Owner, then one email is sufficient.*
b. The *EISG federal employee* saves a copy of the email in the CISO shared *Attestation* folder and updates the *Attestation Tracking Spreadsheet*.	*The* Attestation Tracking Spreadsheet *is an internal document for the use of EISG and is available on the EISG organizational share drive.*
2. After the *EISG federal employee* receives the hard copy of the *Annual Attestation Memorandum*, he/she enters the dates from the memorandum into the *Attestation Tracking spreadsheet*.	
3. After entering in the information, the *EISG federal employee* notifies the *EISG reviewer* that a system is ready for an attestation review.	

PROCEDURE	PRINCIPLE
4. Using the *Attestation Review Checklist*, the EISG reviewer confirms that the information in the memorandum is correct and that the current *CMS Annual Attestation Procedure* was followed.	*The* Attestation Review Checklist *is available in* Appendix B *of this document. If the* CMS Annual Attestation Procedure *was followed correctly, all of the required system information will be up-to-date and will be entered into CFACTS.*
5. Log into CFACTS using RMH Volume II, Procedure 1.1, *Accessing the CFACTS*.	
6. 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.*
7. Click on the *Reports* Tab.	
8. Click on the link for the *System Summary Report*, and select the following report options:	
a. In the *Security Deliverable* field, select *All*.	
b. Check the *Display POC* checkbox.	
9. Click on the *Run Report* button.	
10. Perform the following check in the applicable report:	
a. Under the *System Description* heading, check the following:	
(1) In the *SDLC Status* field, verify that the correct *SDLC Status* is listed.	*For an annual attestation, it should be listed as* Operational.
(2) In the *System Type* field, verify that the correct *System Type* is listed.	*For an annual attestation, should be listed as* GSS *or* Major Application.
b. Under the *Security Authorization* heading, check the following:	
(1) In the *Status* field, verify that the correct ATO status is listed.	*For an annual attestation, it should be listed as* ATO.

PROCEDURE	PRINCIPLE
(2) In the *Accreditation Letter* field, verify that the field states *Yes*.	*For an annual attestation, it should be listed as* Yes. *This indicates that an* ATO letter *is resident in the CFACTS artifacts. NOTE: This does not reflect that this is the* **correct** *artifact; That must be verified manually.*
(3) In the *Last Security Authorization Date* field, verify that the correct date is listed.	*For an annual attestation, it should be listed as the date the ATO was approved. This date is found on the* ATO letter.
(4) In the *Expiration Date* field, verify that the correct date is listed.	*For an annual attestation, it should be listed as the date the ATO expires. This date is found on the* ATO letter.
c. Under the *Risk Assessments* heading, check the following:	
(1) In the *Status* field, verify that the correct Risk Assessment *Status* is listed.	*For an annual attestation, it should be listed as* Completed.
(2) In the *Artifact* field, verify that the field states *Yes*.	*For an annual attestation, it should be listed as* Yes. *This indicates that a Risk Assessment artifact is resident in the CFACTS artifacts. NOTE: This does not reflect that this is the* **correct** *artifact; That must be verified manually.*
(3) In the *Last RA Date* field, verify that the correct date is listed.	*For an annual attestation, this date is* ***after*** *June 10 of the previous year and matches the date on the* Annual Attestation Memorandum. *This date will be available in the Review Log of the current IS RA (if a current FISMA system) or the date on the title page (if a new FISMA system).*
d. Under the *System Security Plan* (SSP) heading, check the following:	
(1) In the *Status* field, verify that the correct System Security Plan *Status* is listed.	*For an annual attestation, it should be listed as* Completed.
(2) In the *Artifact* field, verify that the field states *Yes*.	*For an annual attestation, it should be listed as* Yes. *This indicates that a SSP artifact is resident in the CFACTS artifacts. NOTE: This does not reflect that this is the* **correct** *artifact; That must be verified manually.*

PROCEDURE	PRINCIPLE
(3) In the *Reviewed This Year Date* field, verify that the correct review date is listed.	*For an annual attestation, this date is* ***after*** *June 10 of the previous year and matches the date on the* Annual Attestation Memorandum. *It should be consistent with the date listed in the* Review Log *within the SSP.*
(4) In the *SSP Completion Date* field, verify that the correct date is listed.	*For an annual attestation, it should be listed as the date on the cover of the SSP.*
e. Under the *Security Control Assessment* heading, check the following:	
(1) In the *Status* field, verify that the correct Security Control Assessment *Status* is listed.	*For an annual attestation, it should be listed as* Completed.
(2) In the *SCA Artifact* field, verify that the field states *Yes*.	*For an annual attestation, it should be listed as* Yes. *This indicates that a* Security Assessment **Report** *artifact is resident in the CFACTS artifacts. NOTE: This does not reflect that this is the* **correct** *artifact; That must be verified manually.*
(3) In the *Last SCA Date* field, verify that the correct date is listed.	*For an annual attestation, this date is* ***after*** *June 10 of the previous year and matches the date on the* Annual Attestation Memorandum. *It should be listed as last day of testing given in the* Final SAR *report.*
(4) In the *SAR Artifact* field, verify that the field states *Yes*.	*For an annual attestation, it should be listed as* Yes. *This indicates that a* Security Assessment **Plan** *artifact is resident in the CFACTS artifacts. NOTE: This does not reflect that this is the* **correct** *artifact; That must be verified manually.*
(5) In the *Next SCA Date* field, verify that the correct date is listed.	*For an annual attestation, it should be listed as* ***no later than 60-days before*** *the expiration of the existing ATO.*

PROCEDURE	PRINCIPLE
f. Under the *E-Authentication* heading, check the following:	
(1) In the *Status* field, verify that the correct E-Authentication *Status* is listed.	*For an annual attestation, it should be listed as* ***something other than*** Not Applicable.
(2) In the *Artifact* field, verify that the field states *Yes*.	*For an annual attestation, it should be listed as* Yes. *This indicates that an E-Authentication assessment worksheet is resident in the CFACTS artifacts. NOTE: This does not reflect that this is the* **correct** *artifact; That must be verified manually.*
(3) In the *E-Authentication Completion Date* field, verify that the correct date is listed.	*For an annual attestation, the date should be consistent with the latest system development process (either new or major change.)*
(4) In the *E-Auth Level* field, verify that the correct E-Authentication level is listed.	
g. Under the *Security Categorization* heading, check the following:	
(1) In the *Security Category* field, verify that the correct *Security Category* is listed.	*For an annual attestation,* TBD *is not an acceptable response.*
(2) In the *Security Categorization Date* field, verify that the correct date is listed.	*For an annual attestation, the date should be consistent with the latest system development process (either new or major change.)*
h. Under the *Annual Assessment* heading, check the following:	
(1) In the *Status* field, verify that the correct Annual Assessment *Status* is listed.	*For an annual attestation, it should be listed as* Completed.
(2) In the *Annual Assessment Artifact* field, verify that the field states *Yes*.	*For an annual attestation, it should be listed as* Yes. *This indicates that an* Annual Attestation Memo *is resident in the CFACTS artifacts. NOTE: This does not reflect that this is the* **correct** *artifact; That must be verified manually.*

PROCEDURE	PRINCIPLE
(3) In the *Last Annual Assessment Date* field, verify that the correct date is listed.	*For an annual attestation, it should be listed as no earlier than June 10 of last year. The date matches the date of the* Annual Attestation Memo.
(4) Determine the Security Control Effectiveness and percentage of controls not compliant with the ARS in CFACTS.	
(a) In the *Controls Fully Satisfied* field, click *view* to see the number of controls that are fully satisfied.	
(b) In the *Controls Partially Satisfied* field, click *view* to see the number of controls that are not satisfied.	
(c) In the *Controls Not Satisfied* field, click *view* to see the number of controls that are fully satisfied.	
(d) To determine the percentage of controls not compliant, add the number of not satisfied and partially satisfied controls, and then divide the sum by the total number of controls.	*A high percentage of non-compliant controls may indicate that the security control assessment test results have not been entered in CFACTS in accordance with the applicable RMH Volume II procedure.*
i. Under the *Point of Contact* heading, check the following:	
(1) Verify that each POC listed on the current *Annual Attestation Memo* is reflected correctly in the listed *Points of Contact.*	*For an annual attestation, the Business Owner, System Developer/Maintainer, and the Information System Security Officer must be listed.*
(2) Verify that each POC listed on the current *Annual Attestation Memo* has an email address listed in the *Points of Contact.*	

PROCEDURE **PRINCIPLE**

11. If any of the above information is missing or incorrect, perform the following:

a. Contact the applicable ISSO and have the CFACTS data corrected in accordance with the applicable RMH Volume II procedure.

2.2.3.2 DOCUMENTATION REVIEW

1. Using the *Attestation Review Checklist*, the *EISG reviewer* performs a more in-depth review of the system information and verifies that the current *CMS Annual Attestation Procedure* was followed.

The Attestation Review Checklist *is available in* Appendix B *of this document. If the* CMS Annual Attestation Procedure *was followed correctly, all of the required system information will be up-to-date and will be entered into CFACTS.*

2. Verify all control implementation descriptions in the *Security Controls* Tab in CFACTS as follows:

a. In CFACTS, for the applicable system, perform the following:

(1) Click on the *Reports* tab.

(2) Click on the *Security Controls Report* link.

(3) Select the following parameters:

(a) In the *Control Title* field, select *All*.

(b) Check the *Common Control* checkbox, and select *All* for the field value.

(c) In the *Control Implementation Status* field, select *Undefined*.

Will return controls where the Status *(*In-Place, Planned, Partially In Place*) has not been assigned. Note: The **only** acceptable response is* In Place. *However, this report will only return those with no response at all.*

PROCEDURE	**PRINCIPLE**
(4) Click on the *Run Report* button.	*Creates the report.*
(5) If ***ANY*** controls, with *Yes* in the *Control Applicable?* field, are returned in this report, contact the applicable ISSO and have the CFACTS data corrected in accordance with Procedure 4.2, *Documenting Security Controls in CFACTS.*	*Records returned in this report indicate that the* Control Implementation Status *field was not completed for these controls.*
(6) Click the *here* link at the top of the screen to *return to the previous report*.	*Returns to the* Security Controls Report *screen.*
b. On the *Security Controls Report* screen, select the following parameters:	
(1) In the *Control Title* field, select *All*.	
(2) Check the *Common Control* checkbox, and select *All* for the field value.	
(3) In the *Compliance Description* field, select *Empty*.	*Will return controls without* Control Compliance Descriptions.
(4) Click on the *Run Report* button.	
(5) If ***ANY*** controls are returned in this report, contact the applicable ISSO and have the CFACTS data corrected in accordance with Procedure 4.2, *Documenting Security Controls in CFACTS.*	*These are controls where no compliance description has been provided. This will include inherited controls as well; but inherited controls still need descriptions explaining what portions of the common controls are inherited, how they are inherited, and any remaining system-specific portions that are required.*
(6) Click the *here* link at the top of the screen to *return to the previous report*.	
3. Verify that the *Security Control Assessment Report* indicates that the proper number of controls were tested since June 10 of last year.	

PROCEDURE	PRINCIPLE
4. Verify that the security control assessment test results have been entered into CFACTS.	
a. Click on the *Reports* tab.	
b. Click on the *Security Control Assessment Matrix* link.	*This report displays the security control assessment test results and indicates if the results have been entered in CFACTS.*
c. Check the *Include Inherited Controls* checkbox.	
d. Click on the *Export* button.	*Creates the report.*
e. From the *Export Status* screen, click on the link for the file name with the correct timestamp.	
f. Click *Open* to view the SCA Matrix file.	
g. Under the *Test Date* column, perform a *Find all* to determine the number of control test cases that were performed for this fiscal year and for each of the two previous years.	
h. If test results have not been entered, contact the applicable ISSO and have the CFACTS data corrected in accordance with Procedure 5.6, *Documenting Security Control Effectiveness in CFACTS.*	*The remainder (or portions) of this procedure may be completed first (if possible) to determine if additional corrective actions may also be necessary.*
5. In the *Security Authorization* tab, verify that the *Contingency Plan (CP)* information in the *Contingency Plan* section is correct.	
a. Verify that the *CP Status* field is *Tested.*	*For an annual attestation, it should be listed as* Tested.
b. Verify that the *CP* is in the *1* (or topmost) position, the *CP Test Report* is in the *2* (or next topmost) position, and the *CP Certification* page is in the *100 or next topmost* position.	

PROCEDURE	PRINCIPLE
c. In the *Last CP Completion Date* field, verify that correct date is listed.	*For an annual attestation, this date is* ***after*** *June 10 of the previous year and matches the date on the* Annual Attestation Memorandum. *The Last CP Completion Date is the date in the CP review log and may be after the CP Test date. This is fine as the CP may have been updated after the CP test.*
d. In the *Last CP Test Date* field, verify that the correct date is listed.	*For an annual attestation, this date is* ***after*** *June 10 of the previous year and matches the date on the* Annual Attestation Memorandum. *The Last CP Test Date is the date listed for the CP test in the CP Test Report. If using a datacenter disaster recovery test as their CP test, then it is only valid if the entire system is brought back with the test. If it is only the data that is recovered, then a test has not occurred.*
e. Verify that the CP Certification Page has been signed by the Business Owner.	
f. Verify that any unresolved failures identified in the *CP Test Report*, are listed in the *POA&M* tab in CFACTS and the IS RA.	
6. In the *Security Authorization* tab, verify that the *Privacy Impact Assessment (PIA)* information in the *Privacy Impact Assessment* section is correct.	
a. Verify that the *PIA Status* field is *Completed.*	*For an annual attestation, it should be listed as* Completed.
b. Verify that the *PIA* is in the *1* (or topmost) position, and the HHS *PIA* screenshot is in the *100 or next topmost* position.	
c. In the *Last PIA Date* field, verify that correct date is listed.	*For an annual attestation, this date is* ***after*** *June 10 of the previous year and* ***prior*** *to May 5 of the current year*.

PROCEDURE	PRINCIPLE
7. Verity that the *IS RA* contains the weaknesses from the last SCA.	
8. Verify that POA&M items up-to-date in CFACTS. If not, perform the following:	
a. Review and update as necessary POA&M information in accordance with RMH Volume II, Procedure 6.2, POA&M Management.	
9. The EISG reviewer adds any additional comments to the *Comments* section of the *Attestation Review Checklist.*	
10. The EISG QA confirms that the information in the *Attestation Review Checklist* is correct.	
11. The EISG QA sends the *Attestation Review Checklist* to the EISG federal employee and updates the *Attestation Tracking Spreadsheet* appropriately.	
12. If the *Attestation Review* determines that the system documentation fails to accurately and reasonably reflect the emplaced security controls and resultant residual risks to the system, the EISG QA completes the *Independent Validation and Verification (IV&V) Email Template.*	*If the* CMS Annual Attestation Procedure *is not followed, the* Independent Validation and Verification Email Template *will be completed and sent to the system* Business Owner. *The template is an internal document for the use of EISG and is available on the EISG organizational share drive. Each email will provide details of the deficiencies. The systems will have 30 days to provide the necessary changes or updates.*
a. *EISG QA* completes the *Independent Validation and Verification Email Template* with the pertinent information for the system and sends it to the *EISG federal employee*.	*If there are multiple IV&Vs for one business owner, then one email is sufficient.*
b. The *EISG federal employee* verifies the information in the email and sends it to the *Business Owner*.	

PROCEDURE **PRINCIPLE**

c. The *EISG federal employee* saves a copy of the email in the CISO shared *Attestation* folder and updates the *Attestation Tracking Spreadsheet*.

The Attestation folder is only available to EISG.

2.2.3.3 EISG PACKAGE REVIEW

1. Once *EISG* is notified that a system has completed updates or after the 30 day review period has expired, the *EISG reviewer* uses the *Attestation Review Checklist* to confirm that all the required documentation has been completed, updated, or revised.

If a system receives an Independent Validation and Verification Email*, the system has 30 days to review and provide updates to the information. The system must notify* EISG *when the updates are completed.*

a. If the necessary changes have been completed, the attestation is complete, and either *EISG QA* or the *EISG federal employee* updates the *Attestation Tracking Spreadsheet*.

b. If the necessary changes have not been completed:

(1) Either *EISG QA* or the *EISG federal employee* updates the *Attestation Tracking Spreadsheet*.

(2) The *EISG reviewer* uses the *POA&M Creation* procedure below to create POA&Ms for the system.

2.2.3.4 POA&M CREATION

1. The *EISG reviewer* enters the system's weaknesses into the *SCA Final Findings Spreadsheet* template.

The SCA Final Findings Spreadsheet *is an internal document for the use of EISG and is available on the EISG organizational share drive.*

2. The *EISG reviewer* sends the spreadsheet to *EISG QA*.

PROCEDURE	PRINCIPLE
3. *EISG QA* confirms that all the POA&M items are valid and are not currently outstanding POA&M items in CFACTS.	
4. *EISG QA* sends the spreadsheet to the *POA&M federal employee*.	
5. *EISG QA* fills in the *POA&M Email Template* with the pertinent information for the system and sends it to the *EISG federal employee*.	*The* POA&M Email Template *is an internal document for the use of EISG and is available on the EISG organizational share drive. If there are multiple system POA&Ms for one Business Owner, then one email is sufficient.*
a. The *EISG federal employee* saves a copy of the email in the CISO shared *Attestation* folder.	*The Attestation folder is only available to EISG.*
6. The *POA&M federal employee* uploads the spreadsheet into CFACTS.	
7. The *POA&M federal employee* notifies the *POA&M team member* that there are findings that need weaknesses created.	
8. The *POA&M team member* creates the weaknesses from the uploaded findings and notifies the *EISG federal employee*.	*The POA&M federal employee may also be able to do this step.*
9. The *EISG federal employee* sends the *POA&M Email* from Step 5to the ISSOs and Security POCs.	
10. The *EISG federal employee* marks the system in the *Attestation Tracking Spreadsheet* as complete.	

3 APPROVED

Teresa Fryer

Digitally signed by Teresa Fryer
DN: cn=Teresa Fryer, o, ou,
email=teresa.fryer@cms.hhs.gov,
c=US
Date: 2014.02.03 15:29:09 -05'00'

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.