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 4.2

Documenting Security Controls in CFACTS

FINAL
Version 1.00
February 13, 2012

Document Number: CMS-CISO-2012-vII-pr4.2

(This Page Intentionally Blank)

SUMMARY OF CHANGES IN *DOCUMENTING SECURITY CONTROLS IN CFACTS*, VERSION 1.00

1. Baseline Version

(This Page Intentionally Blank)

TABLE OF CONTENTS

(This Page Intentionally Blank)

1 OVERVIEW

1.1 PURPOSE

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

- Documenting security control implementations for a system in CFACTS.
- Setting up a system in CFACTS to inherit controls from another system in CFACTS.
- Setting up a system to allow *other* systems in CFACTS to inherit its control implementations.

1.2 OTHER RELEVANT PROCEDURES

Other relevant procedures include:

- RMH Volume II, Procedure 1.1, *Accessing the CFACTS*. This procedure is required to gain access to, and log into the CFACTS.
- RMH Volume II, Procedure 5.6, *Documenting Security Control Effectiveness in CFACTS* relies on this procedure to document the security control within the CFACTS before testing can be documented in CFACTS.
- 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 7.3, *CMS Annual Attestation Procedure* relies on this procedure to ensure that all security controls are documented properly and recorded in CFACTS as a prerequisite for submitting an annual attestation.

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

2 SECURITY CONTROL DOCUMENTATION PROCEDURE

PROCEDURE	PRINCIPLE
2.1 DOCUMENTING SECURITY CONTROLS	
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. User has authorized access to the applicable CMS system in CFACTS.	*Some user roles may not have the necessary access rights to enter certain information into CFACTS. Contact the OCISO at mailto:ciso@cms.gov with questions regarding user roles and their access limits.*
a. Refer to RMH Vol II, Procedure 1.1, *Accessing the CFACTS*, for further guidance on gaining authorized access to CFACTS.	
2.1.3 DOCUMENTING SECURITY CONTROLS PROCEDURE	
1. Log into CFACTS using RMH Volume II, Procedure 1.1, *Accessing the CFACTS*.	
2. Click on the link for the applicable system from either the *Home* screen or the *Browse* Screen.	*Opens the applicable system to the* Identification *tab.*

PROCEDURE	PRINCIPLE
3. Select the *Security Controls* tab.	*Enables the* Security Controls *tab on the* Self-Assessment *screen.*
4. If not already in *Tree View* mode, select *Tree View* to *On.*	Tree View *in the* On *setting will display a listing of the Security Control requirements on the left side of the screen.*
5. Navigate to the applicable *Security Control* by selecting the applicable control from the listing on the left side of the screen.	*Users may also navigate by using the* First, Previous, Next, *and* Last *links at the top and bottom of the page.*
6. To see the **full** text of the control requirement:	
a. Click on the *more details* link within the *Description* field.	*Opens the* Security Controls *screen and details the applicable ARS* Baseline Requirement, Implementation Standard(s), *and* Enhancement(s) *that must be met by the control implementation.*
b. Click the *Close* button when finished with the full text.	*Returns to the* Self-Assessment *screen.*
7. For the *Security Control Scoping* field, leave this field as assigned by CFACTS.	*The default values are as assigned by NIST based on the security impact level of the system. If a business owner feels that these values should be modified, contact the OCISO at mailto:ciso@cms.gov.*
8. If this is an inheritable control, click on the *alert* link in the *Common Control* field:	*For controls that are inherited from a control provider, this field will be populated automatically.*
a. Verify that any *alerts* are understood and addressed.	*Alerts are issued when Common Controls information changes. If any information supplied by the common control provider has been changed, it will be indicated in an* alert. *Inheritors of common controls should read and understand all* alerts. *If the information provided in the alert indicates a material change to the implementation or effectiveness of the provided control, the inheritor must take action to adjust the system-specific implementation to address the change in the control provider implementation.*

PROCEDURE	PRINCIPLE
b. For the *Common Control* field, leave this field as populated by CFACTS.	*This is the information provided by the* common control provider. *Inheriting systems have no influence, control, or rights to modify this information.*
9. For the *Control Implementation Status* field, check the *In Place* checkbox.	*FISMA systems seeking or maintaining an ATO can* ***only*** *have controls that are* In Place. *Any FISMA system with controls that are not* In Place, *as designed, should not be put into service. For systems still in a non-*Operational *phase of the system development life-cycle (as documented on the* System Identification *tab*—SDLC Status *field), controls will be understood to be in a* less-than-fully-implemented, *and non-operational state. Therefore, it is* ***not*** *necessary to check the* Planned *or* Partially In Place *checkboxes for system not on the* Operational *SDLC phase.*
10. For the *Security Controls Effectiveness* field, leave as populated by CFACTS.	*This field is populated by CFACTS based on the* Security Control Assessment *results. Under* **NO** *circumstances select* **ANY** other *values* manually.
11. For the *Risk Based Decision* field, leave as populated by CFACTS.	
12. For the *Inherited From* field, leave as populated by CFACTS.	

PROCEDURE	PRINCIPLE
13. Populated the *Compliance Description* field as follows:	
a. Describe how the *system* achieves compliance with the *Baseline Control*, all of the *Implementation Standards*, and each listed *Enhancement*:	
NOTE ***FULLY-inheritable*** **controls do not require additional implementation at the *System-Specific* level. If an inherited control requires ANY management or configuration at the *system-specific* level to implement, then it is NOT considered to be *FULLY*-inheritable.**	*Fully-inheritable control effectiveness **cannot** be influenced by individual systems. If an individual 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 testing be required at the system-specific level to ensure that the control is implemented at its full effectiveness.*
(1) If the *Inherited From* field does **not** say *"Not Applicable"*, perform the following:	*The* Inherited From *field indicates the system(s) from which this control is inherited.*
(a) Explain what portion of the control described in the *Common Control* field is being inherited.	*The description provided by the common control provider may include some capabilities that are not used by the local system (such as inheritable* mainframe RACF *capabilities that might not be applicable to a local mid-tier* Active Directory *–based system.)*
(b) Explain any *system-specific* configurations or administrative processes are required to implement the inherited control.	*For example: If an inherited control requires that a local system be configured to utilize* Active Directory *as an access control method, explain how this was configured and is managed during the life-cycle.*
(c) Explain what portion of the control requirement is remaining that must be addressed by a *system-specific* control implementation.	*For example: A common control provider may provide overall user identity management services for user-level* application *access. However, it may* **not** *provide those services for local Administrator-level access control to virtual servers or other local hardware. Explain how the system-specific control implementation addresses these shortcomings.*

PROCEDURE	PRINCIPLE
(2) Describe ***how*** the objectives of the requirements, **including all applicable *Implementation Standards***, are being achieved.	*For operational systems, do not include* planned *controls or controls that are* not fully implemented *as the basis for compliance. This description should only include controls as they are currently implemented.*
(3) Describe ***where*** any associated *processes* and *procedures* are maintained.	
(4) Describe ***who*** is the responsible party for ensuring that this control is being properly implemented.	*This must be a person associated with the* current *system, NOT a person outside of the business owner's organization or at a common control provider's organization. It may be a* contractor*, but should **also** designate the CMS responsible party for directly managing that contractor.*
(5) Describe any *additional* controls that may be planned **and the proposed dates of implementation** in the operational environment.	
14. For the *Compliance Details* field, upload any necessary documentation as follows:	*Upload any additional documentation necessary to describe or understand the implementation of the controls for this requirement.* ***Any current approved*** **Risk Acceptance** ***forms for this control are REQUIRED to be uploaded.***
a. To add *new* documentation perform the following:	
(1) Click on the *New* link.	*Opens the* Add Description *screen.*
(2) In the *Title* field, enter a title for the document to be uploaded.	
(3) In the *Description* field, enter a description for the document to be uploaded.	*It is the* Description *(not the* Title*) that will be displayed on the Self-Assessment form, so be concise.*
(4) Click on the *Save* button.	*Returns to the* Self-Assessment *screen.*
(5) In the *Compliance Detailed* field, click on the *Upload* link for the entry just created.	*Opens the* Upload Support Document *screen.*

PROCEDURE	PRINCIPLE
(6) Click on the *Browse* button to navigate to and select the applicable file to upload.	
(7) Select the applicable *Artifact Type* (*Text* or *Image*) as appropriate.	*For images (JPEG, PNG, and BMP files are supported), select* Image, *or all others select* Text.
(8) Click on the *Upload* button.	
(9) Click the Close button.	*Returns to the* Self-Assessment *screen.*
b. To *update existing* documentation perform the following:	
(1) In the *Compliance Detailed* field, click on the *Upload* link for the applicable entry to be updated.	*Opens the* Upload Support Document *screen.*
(2) Click on the *Browse* button to navigate to and select the applicable file to upload.	
(3) Select the applicable *Artifact Type* (*Text* or *Image*) as appropriate.	*For images (JPEG, PNG, and BMP files are supported), select* Image, *or all others select* Text.
(4) Click on the *Upload* button.	
(5) Click the Close button.	*Returns to the* Self-Assessment *screen.*
15. For the *Compensating Control* field, leave as populated by CFACTS.	
16. Click on the *Save* button.	
17. Perform ***one*** of the following:	
a. To document additional control implementations, return to Step 5, ***or***	
b. Exit this procedure.	

PROCEDURE	PRINCIPLE
2.2 INHERITING SECURITY CONTROLS	
2.2.1 PROCEDURE USERS	
1. CMS Information System Security Officer (ISSO).	
2. Business Partner System Security Officer (SSO).	
3. Designated CFACTS data entry person.	
2.2.2 INITIAL CONDITIONS	
1. User has authorized access to the applicable CMS system 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.*
2. Refer to RMH Vol II, Procedure 1.1, *Accessing the CFACTS*, for further guidance on gaining authorized access to CFACTS.	
2.2.3 INHERITING CONTROLS PROCEDURE	
1. Log into CFACTS using RMH Volume II, Procedure 1.1, *Accessing the CFACTS*.	
2. Select the applicable system from either the *Home* screen or the *Browse* Screen.	*Opens the applicable system to the* Identification *tab.*
3. Select the *FIPS 199* radio button.	*Accesses the* Security Categorization *and* Common Control Management *portions of the* Identification *tab.*

PROCEDURE	PRINCIPLE
4. To *add* a new common control provider to the list, perform the following:	
a. Click on the *Manage Common Control Access* link.	*Opens the* Manage Common Control Access *screen.*
b. Select the *Add Common Control Providers* radio button.	*This selection allows you to* receive *common controls from a system that has granted access to this system to* consume *their common controls.*
c. For each common control provider to *ADD*, perform the following:	
(1) Select the applicable common control provider from the *System/Site/Program* dropdown menu.	*Only common control providers that have specifically* authorized *this system to* consume *their shared controls will be displayed on the dropdown list. If a desired common control provider is not listed, contact the applicable ISSO for the common control provider system and request access to be granted as a consumer of common controls from their system.* *If nothing is listed in the System/Site/Program, then no common control providers are available to the applicable system. Contact the office of the CISO at mailto:ciso@cms.gov if this has occurred, and you believe it is in error.*
(2) Click on the *Add* button on the *Manage Common Control Access* screen.	*This action should open a verification screen that indicates success.*
(3) Click *Close* on the verification screen.	*Closes the verification screen and returns the user to the* Manage Common Control Access *screen.*
(4) Check/verify the desired common control provider has been added to the list.	
(5) Click *Close* on the *Manage Common Control Access* screen.	*Returns to the* Identification *screen.*

PROCEDURE	PRINCIPLE
5. To *remove* a common control provider from the list, perform the following:	
a. Verify that all controls provided by this provider are **NOT** being used:	
(1) Click *Receive Common Control.*	*Opens the* Receive Common Control *screen*.
CAUTION **For any control(s) being changed from *Inherited* to *None*, the applicable control implementation response will need to be updated to reflect that the control is no longer being inherited.**	*If this is the case, **each** applicable control implementation description should be **immediately** updated in accordance with Section 2.1,* Documenting Security Controls, *and re-tested at the earliest available assessment.*
(2) For each *Control Family* for the applicable common control provider, select (or verify selected) the *None* radio button.	*Deselect those controls and removes applicable inheritance of controls from that provider.*
(3) Click *Save* on the *Receive Common Control Access* screen.	
(4) If changes were made, click through verification page by clicking on the *Continue* button.	*If this is the case,* all *applicable control implementation descriptions will be **immediately** updated to reflect the removal of inheritance from that provider.*
(5) Click *Close* on the *Receive Common Control Access* screen.	*Closes the* Receive Common Control Access *screen.*
(6) Click the *Manage Common Control Access* link.	*Opens the* Manage Common Control Access *screen.*
(7) Click the *Delete* link next to the applicable common control provider that you wish to remove from the list.	*If controls are still being shared, an error message will be presented. If this occurs, return to Step a.*
(8) Click *Close* on the verification screen.	*Closes the verification screen and returns the user to the* Manage Common Control Access *screen.*
(9) Click *Close* on the *Manage Common Control Access* screen.	*Closes the* Manage Common Control Access *screen*

PROCEDURE	PRINCIPLE
6. To receive or verify specific common control(s) from a common control provider, perform the following:	
a. Select *Receive Common Control.*	*Opens the* Receive Common Control *screen.*
b. For each applicable *Control Family*, perform the following:	
NOTE **Do NOT select *"Inherited"* for an entire Control Family.**	*Each **individual** control must be evaluated before it can be determined if it* **should** *be inherited. While some controls may be listed as "inheritable", if they cannot be implemented as described/designed by the control provider, then they should **not** be inherited.*
(1) Click on the adjacent *"X"* to expand the applicable *Control Family*.	
(2) For each control available for inheritance in the applicable *Control Family*, determine if each control in the list should (or can) be inherited for the applicable system.	
(3) For each listed control that has been determined to be *inherited*, select the *Inherited* radio button under the applicable control provider column.	*Note that the same control may be inherited from MULTIPLE providers. If that is the case, then ALL providers must be fully-assessed at a* Passed *level before the control may be considered as* Fully Satisfied.
(4) For each control that has been determined to be *NOT inherited*, select the *None* radio button.	
(5) Click *Save on* the *Receive Common Control* screen.	*Saves all changes to the* Receive Common Control *screen.*
(6) Click *Close* on the *Receive Common Control* screen.	*Closes the* Receive Common Control *screen and returns the user to the* FIPS 199 *screen on the* Identification *tab.*

PROCEDURE	PRINCIPLE
2.3 SHARING INHERITABLE CONTROLS	
2.3.1 PROCEDURE USERS	
1. CMS Information System Security Officer (ISSO).	
2. Business Partner System Security Officer (SSO).	
3. Designated CFACTS data entry person.	
2.3.2 INITIAL CONDITIONS	
1.	
2.3.3 SHARING INHERITABLE CONTROLS PROCEDURE	
1. Log into CFACTS using RMH Volume II, Procedure 1.1, *Accessing the CFACTS*.	
2. Select the applicable system from either the *Home* screen or the *Browse* Screen.	*Opens the applicable system to the* Identification *tab.*
3. Select the *FIPS 199* radio button.	*Accesses the* Security Categorization *and* Common Control Management *portions of the* Identification *tab.*
4. Click on the *Define Common Control* link.	*Opens the* Define Common Control *screen.*
5. For each *Control Family* of controls that contain controls to be shared, perform the following:	
a. Click on the adjacent *"X"* to expand the applicable *Control Family.*	

PROCEDURE	PRINCIPLE
b. For each control that is to be made available for inheritance in the applicable *Control Family*, select or verify-selected the *Enabled* radio button.	*Clicking on* Enabled *allows authorized systems to inherit that control from the current system.*
6. For each control that is ***NOT*** to be shared for inheritance in the applicable *Control Family*, select or verify-selected the *None* radio button.	*Clicking on* None *prevents any system from inheriting that control from the current system.*
7. Click on the *Save* button on the *Define Common Control* screen.	*Saves the changes made.*
8. Click on the *Close* button on the *Define Common Control* screen.	*Closes the* Define Common Control *screen.*

2.4 DOCUMENT SYSTEM INTERCONNECTIONS

2.4.1 PROCEDURE USERS

1. CMS Information System Security Officer (ISSO).

2. Business Partner System Security Officer (SSO).

3. Designated CFACTS data entry person.

4. OCISO Staff.

2.4.2 INITIAL CONDITIONS

1. User has authorized access to the applicable CMS system in CFACTS.	*Some user roles may not have the necessary access rights to perform this procedure in CFACTS. Contact the OCISO at mailto:ciso@cms.gov with questions regarding user roles and their access limits.*
a. Refer to RMH Vol II, Procedure 1.1, *Accessing the CFACTS*, for further guidance on gaining authorized access to CFACTS.	

PROCEDURE	PRINCIPLE
2. The applicable system interconnections have been identified and applicable *Interconnection Security Agreement (ISA), Service Level Agreement (SLA),* or *Memorandum of Understanding (MOU)* have been established and documented.	
2.4.3 DOCUMENT SYSTEM INTERCONNECTIONS PROCEDURE	
1. Log into CFACTS using RMH Volume II, Procedure 1.1, *Accessing the CFACTS*.	
2. Click on the link for the applicable system from either the *Home* screen or the *Browse* Screen.	*Opens the applicable system to the* Identification *tab.*
3. Click on the *People and Inventory* tab.	
4. Select the *Interconnections* radio button.	
5. Perform ***one*** of the following:	
a. On the *List of Interconnections,* click on *Edit,* ***or***	*Opens the* Edit Interconnections *screen to modify an existing interconnection.*
b. On the *List of Interconnections,* click on *New* and perform the following:	*Opens the* Add Interconnections *screen to add a new interconnection.*
(1) For the *Component* field, select from the dropdown the applicable *Component* for the applicable system for which an interconnection is being documented.	*The* Component *field should reflect the CMS component that is required to have this interconnection to conduct its business or service its particular constituency. This should reflect the Business Owner component, not the System Maintainer's.*
(2) For the *System Name* field, perform ***one*** of the following:	
(a) If the connection is to an *internal* CMS system, select from the dropdown the applicable CMS *System Name* to which the interconnection is being documented, ***or***	*For an interconnection with an* internal *CMS FISMA system, select that system from the dropdown list. If the system is not listed, immediately contact the OCISO at mailto:ciso@cms.gov.*

PROCEDURE	PRINCIPLE
(b) If the connection is to an *external* system, proceed as follows:	*An* external *system is defined as a non-CMS system.*
i. Select *Not Applicable* from the dropdown list.	
ii. For the *Organization Name* field, provide the name of the *external* organization that is being connected.	*Example: "International Bank of North America – Manhattan Branch"*
iii. For the *Interconnection Name* field, provide a short descriptive name for the interconnection.	*Example: "External IBNA payment account via T1 line"*
6. For the *Type* field, provide a short description of how the connection is established.	*Example: "FIPS 140-2 compliant VPN over the CMS MPLS network"*
7. For *internal* connections:	
a. For the *Security Category* field, maintain as populated by CFACTS.	*This information is populated from the internal system data maintained in CFACTS for the interconnected system.*
b. For the *SA&A Status* field, maintain as populated by CFACTS.	*This information is populated from the internal system data maintained in CFACTS for the interconnected system.*
8. For *external* connections:	
a. For ***interconnections to other FISMA systems*** maintained and authorized outside of CMS, perform the following:	*These are FISMA systems whose ATO is granted and maintained by some other Federal Agency.*
(1) For the *Security Category* field, select the applicable FIPS 199 security level for the interconnected system.	
(2) For the *SA&A Status* field, select the applicable *SA&A Status* (ATO status) for the interconnected system.	
b. For ***interconnections to non FISMA systems***, perform the following:	*Non-FISMA systems are* ***not*** processing, transmitting, *or* storing *information on behalf of* ***any part*** *of the Federal government.*
(1) For the *Security Category* field, select *Undefined*.	

PROCEDURE	PRINCIPLE
(2) For the *SA&A Status* field, select *Not Applicable*.	
NOTE: **Responses for *Validate External Interconnection* of *Undefined* are NOT allowed at CMS.**	
9. For the *Validate External Interconnection* field, select either *Yes* or *No*.	*This field indicates whether the interconnection* **path** *(physical or virtual network) has been* explicitly *tested (from end-to-end) for meeting CMS security requirements.*
10. For the *Contractor Operation of Facility* field, perform ***one*** of the following:	
a. Select ***No*** if the system being connected to 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 ***Yes*** for ***all*** others.	
11. For the *Contractor Operation of Facility* field, perform ***one*** of the following:	*The system's boundaries are tested in the Security Controls Assessment (SCA). If all controls passed, then select yes.*
a. If ***all*** of the boundary controls within the system ***and*** the interconnection path were fully tested, and all ***passed***, select *Yes*, ***or otherwise***	
b. Select *No*.	
(1) In the *Planned Action If Not Effective* field, develop **and list** all of the *Weaknesses* created to remediate the identified issues.	
12. Click on the *Save* button.	*Saves the information entered on the* Add Interconnections *screen and returns to the* People and Inventory *screen.*
13. Click on the *Edit* link for the applicable connection.	*Opens the* Edit Interconnection *screen.*

PROCEDURE	PRINCIPLE
NOTE: **An *Interconnection Agreement Type* of *Not Applicable* or *SLA* is NOT allowed at CMS.**	*ALL interconnections **must** be documented by a **security** agreement between the parties responsible for the applicable systems.*
14. Perform ***one*** of the following:	
a. For *internal* connections:	
(1) For the *Agreement Type* field, select *MOU*.	*A* Memorandum of Agreement (MOU) *is required for all internal connections between systems.*
b. For *external* connections,	
(1) For the *Agreement Type* field, select *ISA*.	*An* Interconnection Security Agreement (ISA) *is required for all external connections to CMS systems.*
NOTE: **An interconnection *Status* of *Not Applicable* is NOT allowed at CMS.**	*ALL interconnections **must** be documented by a **security** agreement between the parties responsible for the applicable systems.*
15. For the *Status* field, select the applicable status of the interconnection agreement.	*Interconnections with internal or external systems are NOT allowed without a current interconnection agreement.*
16. For the *Last Completion Date* field, enter the *Last Completion Date*, for the latest interconnection agreement.	*This date should reflect the date that the latest FINAL interconnection agreement was signed.*
17. For the *Expiration Date* field, enter the *Expiration Date*, for the latest interconnection agreement.	*This date should reflect the date that the latest FINAL interconnection agreement expires.*
18. For the *Next Completion Date* field, enter the *Next Completion Date*, for the latest interconnection agreement.	
19. Upload the latest completed interconnection agreement as follows:	
a. In the *Interconnection Agreement* field, click on the *Upload* link.	*Opens the* Upload Support Document *screen.*
b. Click on the *Browse* button to navigate to and select the applicable file to upload.	

PROCEDURE	PRINCIPLE
c. Click on the *Upload* button.	
d. Click the Close button.	*Returns to the* Edit Interconnection *screen.*
20. For the *Point of Contact* field, perform the following.	
a. Perform ***one*** of the following:	
(1) Click on *New*, ***or***	
(2) Click on *Edit* for a POC to be edited.	
b. In the *Name* field, enter/verify a *Name* for the POC.	
c. For the SA&A Role field, select the applicable *Role* from the dropdown.	
d. For the *HR Title* field, enter the applicable *HR Title* information for the POC.	
e. For the *Organization* field, enter the applicable *Organization* information for the POC.	
f. For the *Address* field, enter the applicable *Address* information for the POC.	
g. For the *Phone* field, enter the applicable business *Phone* number for the POC.	
h. For the *Email* field, enter the applicable *Email* contact information for the POC.	
i. For the *Fax* field, enter the applicable *Fax* number for the POC.	
j. For the *Responsibility* field, enter the applicable *Responsibility* description for the POC.	
k. Click on the *Save* button.	
l. Click on the *Close* button.	*Returns to the* Edit Interconnection *screen.*
21. Click on the *Save* button.	*Saves information and returns to the* People and Inventory *screen.*

PROCEDURE	PRINCIPLE
22. Exit this procedure.	

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 15:43:32 -05'00'

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

This document will be reviewed periodically, but no less than annually, by the Office of the Chief Information Security Officer (OCISO), and updated as necessary to reflect changes in policy or process. If you have any questions regarding the accuracy, completeness, or content of this document, please contact the OCISO at mailto:ciso@cms.gov.

(This Page Intentionally Blank)