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

Risk Management Manual
Volume II
Procedure 1.1
Accessing the CFACTS

FINAL
Version 1.00
April 21, 2011

Document Number: CMS-CISO-201X-vII-pr1.1

(This Page Intentionally Blank)

SUMMARY OF CHANGES IN VOL II, PROC 1.1, *ACCESSING THE CFACTS* VERSION 1.00

1. Baseline Version.

(This Page Intentionally Blank)

TABLE OF CONTENTS

LIST OF TABLES

(This Page Intentionally Blank)

1 OVERVIEW

1.1 PURPOSE

The purpose of this procedure is to establish an authorized user with sufficient access necessary to perform required functions within the CMS FISMA Controls Tracking System (CFACTS). These procedures encompass: 1) establishing a required Enterprise User Administration (EUA) system account, 2) establishing access rights into CFACTS, 3) establishing required rights within the CFACTS to perform assigned duties, and 4) logging into the CFACTS.

Contractors must coordinate through their Government Task Leads (GTLs) or Project Officers (POs) to obtain access. User access requests for CFACTS are routed to the Office of the CMS Chief Information Security Officer (OCISO) for review and approval. Upon approval by OCISO, the CFACTS system administrator adds the user to the application, assigns him/her access to the appropriate systems, and defines their roles within the application.

The process to add both *internal users* (CMS employees and Contractors working onsite) and *external users* (Contractors working offsite for CMS) is the same.

1.2 OTHER RELEVANT PROCEDURES

Completion of this procedure is required prior to performing ***any*** other procedures that include actions within the CFACTS tool.

(This Page Intentionally Blank)

2 ACCESSING THE CFACTS

PROCEDURE

2.1 SETTING UP A CFACTS ACCOUNT

2.1.1 PROCEDURE USERS

1. Prospective CFACTS users as defined in Table 1, *CFACTS Role*.

2.1.2 ENTRY CONDITIONS

1. Prospective user has established web browser access to the CFACTS environment.

2.1.3 INSTRUCTIONS

2.1.3.1 GETTING CFACTS ACCESS THROUGH EUA

1. Complete and sign an EUA request form:

a. Download the latest *Application for Access to CMS Computer Systems* form from http://www.cms.gov/InformationSecurity/Downloads/EUAaccessform.pdf.

b. Complete and sign the request per the applicable procedure located at http://www.cms.gov/InformationSecurity/Downloads/EUA_User_Guide.pdf.

PRINCIPLE

The CFACTS is not a public Internet-facing system. Therefore CMS Intranet (or CMSNet) access is required to access the CFACTS. Contractors should establish necessary connectivity through their applicable CMS Contracting Officer (CO) or Government Task Lead (GTL).

All new CFACTS users must complete this procedure–even if they already have an active EUA account. *This process is required both to acquire a new EUA account and/or to add the appropriate CFACTS Job Code to the user's EUA access rights.*

PROCEDURE

PRINCIPLE

CAUTION

For users with *existing* EUA accounts, ensure requests include appropriate CFACTS job code(s) AND all other EUA Job Codes necessary to perform other assigned duties.

c. In the section labeled *Required Accesses*, include the appropriate Job Code from Table 1.

The Job Code for most business owner or contractor users will be CFACTS_USER_P (ISSO or their support). Contact the OCISO at mailto:ciso@cms.hhs.gov if you are unsure of your appropriate job code.

2. Submit to:

a. **For CMS Employees,** submit request to their CMS Access Administrator (CAA).

List of current CAAs can be found at http://www.cms.gov/InformationSecurity/Downloads/CAAList.pdf.

b. **For Contractor personnel,** submit request to their applicable CMS Contracting Officer (CO) or Government Task Lead (GTL).

(1) CMS CO or GTL submit contractor requests to the applicable CAA.

CO and/or GTL should first verify that the requesting contractor has a valid business and contractual need for the requested access.

2.1.3.2 GETTING ACCESS TO THE APPROPRIATE CFACTS SYSTEM DATA

CAUTION

Contractor-access to competitor system(s) information should be tightly controlled to ensure that *company-proprietary* information is not inappropriately disclosed.

Due to the security sensitivity of the data contained in the CFACTS, users are ONLY granted access to those CMS system(s) necessary for users to perform their assigned duties.

1. After EUA access has been established for the applicable user, perform the following:

PROCEDURE **PRINCIPLE**

a. The applicable CMS ISSO submits an email to the OCISO (mailto:ciso@cms.hhs.gov) requesting access for the applicable user(s), to the applicable system(s). For each request, the ISSO must include:

(1) Applicable EUA User ID(s).

(2) Applicable CFACTS system name(s) for the system(s) for which access is being requested.

ISSOs may request user access ONLY to systems for which they are assigned ISSO responsibilities. If access is required to other systems, not assigned to the applicable ISSO, an additional request must be made by the applicable system ISSO.

2.2 LOGGING INTO THE CFACTS

2.2.1 PROCEDURE USERS

1. Authorized CFACTS users.

2.2.2 ENTRY CONDITIONS

1. User has valid EUA User ID.

2. User has valid CFACTS account.

3. User has established web browser access to the CFACTS environment.

See Section 2.1.3.1 to acquire necessary EUA account.
See Section 2.1.3.2 to acquire necessary CFACTS access.
The CFACTS is not a public Internet-facing system. Therefore CMS Intranet (CMSNet) access is required to access the CFACTS.

2.2.3 CFACTS LOGIN

1. Navigate your web browser to https://cfacts.cms.cmsnet/.

PROCEDURE	**PRINCIPLE**
2. Review the contents, and the warning listed on the log-in page before proceeding into the system.	
3. Enter CMS User ID and password.	*Must be an authorized user. See Section 2.1.*
4. Click *Login*.	
5. Read-and-heed the warning, and click *Enter.*	
6. Most users will now be in the *Home* page (some elevated users will now be at the *Browse* page.)	
7. Proceed to the applicable procedure for performing user duties.	

2.3 TABLES AND FIGURES

Table 1 CFACTS Job Codes

Job Code	Description	CFACTS Role
CFACTS_EXEC_P	Access to this job code will be restricted to OIS Executives (CIO, Deputy CIO, CTO, and CISO) that can see Agency wide Plan of Action & Milestones (POA&Ms) and Security Authorization documentation. This will be a read only access.	OIS Executives
CFACTS_OCISO_P	Access to this job code will be restricted to OCISO security staff responsible for performing system administration functions within the application. This will be a read and write access privileges.	CFACTS System Administrators
CFACTS_COMPONENT_P	Access to this job code will be restricted to Component Head and his/her deputy to view all FISMA systems assigned to their components. This will be a read only access privilege.	Business Owner and his/her Deputy
CFACTS_BUS_MAINT_P	Access to this job code will be restricted to System Developer Maintainers to access all applications they have been assigned. This will be a read and write	System Developer Maintainer
CFACTS_USER_P	Access to this job code will be restricted to ISSOs to access all applications they have been assigned. This will be a read and write access privileges.	ISSOs and System Users
CFACTS_SUPPORT_P	Access to this job code will allow OCISO staff to perform support functions, e.g., helpdesk, troubleshooting, etc., within the application. This will be a read and write access privileges.	CFACTS Support Personnel
CFACTS_PRIVACY_P	Access to this job code will allow Privacy Division employees to enter privacy data into the system. This will be a read and write access.	Privacy Office Personnel
CFACTS_STE_P	Access to this job code will allow the ST&E Coordinator or representative to enter ST&E data into the system. This will be a read only access privilege.	ST&E Coordinators
CFACTS_AUD_P	Access to this job code will provide the Auditor the ability to view POA&M and SA data. This is a read only access privilege.	Auditors

3 APPROVED

Charles R. Brewer

Digitally signed by Charles R. Brewer
DN: c=US, o=U.S. Government, ou=HHS, ou=CMS, ou=People, cn=Charles R. Brewer, 0.9.2342.19200300.100.1.1=2000389294
Date: 2011.04.22 12:54:36 -04'00'

C. Ryan Brewer
CMS Chief Information Security Officer and
Director, Office of the Chief Information Security Officer

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