Federal Facilitated Marketplace (FFM) System

DEPARTMENT OF HEALTH AND HUMAN SERVICES
CENTERS FOR MEDICARE & MEDICAID SERVICES
OIS/EISG
RECORD OF SIGN OFFS

Prepared by: Jerry Oar
Phone: 541-673-9085
Fax No. 703-361-0384

Typed By: Jerry Oar
Phone: 541-673-9085

Disc Identifier: FFM_ATO_ltr_9-26-2013

ACTION	NAME	OFF/DIV/BR	INITIALS/DATE
REVIEWED BY	Jacqueline Toomey	OIS/EISG/DISPC	
REVIEWED BY	Michael Mellor	OIS/EISG	
REVIEWED BY	Teresa Fryer	OIS/EISG	
REVIEWED BY	George Linares	OIS	
CLEARED BY	Tony Trenkle	OIS	

KEYWORD:

COMMENTS: Authorization To Operate form(s) attached for the CMS CIO's signature.

Please Return to Linda Velasco, EISG

Please include the name of someone who we can contact in your absence for questions/information.

Federally Facilitated Marketplaces (FFM)

Executive Summary

There is an **Authorization to Operate (ATO) until March 20, 2014** to allow testing and closure of risk weaknesses in FFM and the supporting infrastructure. The current configuration includes: Qualified Health Plans (QHP), QHP-Dental modules, parts of Plan Management (PM), parts of Eligibility & Enrollment (E&E), and parts of Financial Management (FM).

Authorization Summary:

The following is a review summary of FFM:

- **The independent validation contractor was unable to adequately test the confidentiality and integrity of the FFM system in full.** The majority of the contractor's testing efforts were focused on testing the expected functionality of the application. Complete end-to-end security testing of the FFM application never occurred. Several factors contributed to the limited effectiveness of the SCA.

  The contractor was not able to complete testing because:
  - *Testing environments and module interconnections were not ready for the SCA.*
  - *Valid test data was not provided prior to testing.*
  - *Test environment availability was not consistent.*
  - *Environments were not dedicated to SCA testing.*

Current Security Assessment Status Summary

Contractor	Assessment Status	POA&M (Y/N)
MITRE Blue Canopy	*2 high, 22 moderate and 13 low findings remain open (4/12/2013 MITRE) 3 moderate and 5 low findings remain open (9/19/2013 Blue Canopy) 11 moderate and 8 low findings remain open (9/19/2013 MITRE)	No for the Blue Canopy and the 2nd MITRE tests

Points of Contact (POCs) were confirmed by CFACTS

System Level	Business Owner	Sys Developer/ Maintainer	ISSO
Moderate	James Kerr OA/CMHPO	Mark Oh OIS/CIISG/DHIM	Darrin Lyles OIS/CIISG/DSMDS

Documentation Artifacts

Authorization Request	SSP	RA	CP	CP Test	Security Assessment	PIA
	09/09/2013 Updates Included	09/09/2013 Updates Included	08/05/2013 Not Signed	08/16/2013	*04/12/2013 09/19/2013 MITRE 09/19/2013 Blue Canopy	08/05/2013

There was a FFM ATO memorandum signed and dated September 3, 2013. Although the action items from that ATO are not in CFACTS, they are applicable to this ATO. CIISG did not provide a Certification Form for this current authorization request.

*There are weaknesses listed in CFACTS from the FFM_FFE_SCA_05032013-FFM_FFE-QHP_SCA document. The weakness milestones were disapproved by EISG.

FFM could not be fully assessed during the August and September assessment attempts.

Note: Blue Canopy indicated –"Publically Accessible Data: Using NotResp NotResp data was accessed that should not be publically accessible. We recommend considering the potential security risks from divulging this data and implementing appropriate controls." The incident response (IR) family assessment was not included in the scope of the independent tests. However, a review of the documentation included reviews of the IR family. The System Security Plan incorrectly indicates e-authentication level 2 which provides very little identity proofing to assist in protecting sensitive data and incident investigations.

Federally Facilitated Marketplaces (FFM)

Executive Summary

Recommended Decision:

- **Denial Authorization To Operate (DATO)**. This allows testing and closure of risk weaknesses in FFM and the supporting infrastructure. The current configuration includes only the Federally Facilitated Marketplaces; Qualified Health Plans (QHP), and Dental modules, Plan Management (PM), Eligibility & Enrollment (E&E), My Account, Individual Application, Plan Compare, Eligibility Support Desktop (ESD), Call Center Integration, Direct Enrollment, Federal Functions (Double Dipping), Federal Functions (EDS to store FFM and SBM Transactions), Enrollment, Notices, Mailing Contractor Integration, and Financial Management (FM). Other FFM modules will be added in the future requiring their own Security Control Assessment (SCA).

Authorization Summary:

The following is a review summary of FFM:

- **MITRE was unable to adequately test the Confidentiality and Integrity of the HIX system in full.** The majority of the MITRE's testing efforts were focus on testing the expected functionality of the application. Complete end to end testing of the HIX application never occurred. Several factors contributed to the limited effectiveness of this SCA.

  MITRE was not able to complete testing do to:
  - ***Testing environments and module interconnections were not ready for the SCA.***
  - ***Valid test data was not provided prior to testing.***
  - ***Test environment availability was not consistent.***
  - ***Environments were not dedicate to SCA testing.***

- NotResp

  The presence of high risk findings in a system represents an increased risk to the CMS enterprise. Lifecycle management of the system requires initial testing for FISMA authorization and continuous monitoring. Non-compliance with the *CMS Information Security (IS) Acceptable Risk Safeguards (ARS), CMS Minimum Security Requirements (CMSR)* without continuous monitoring presents an unacceptable risk.

- NotResp

  The presence of high risk findings in a system represents an increased risk to the CMS enterprise. Lifecycle management of the system requires initial testing for FISMA authorization and continuous monitoring. Non-compliance with the *CMS Information Security (IS) Acceptable Risk Safeguards (ARS), CMS Minimum Security Requirements (CMSR)* without continuous monitoring presents an unacceptable risk.

- **All FFM weaknesses in CFACTS are in a delayed status.** Not mitigating the FFM weaknesses weakens the security posture of FFM and the CMS enterprise and as such requires immediate attention to provide the level of protection mandated by CMS.

  FFM weaknesses have twice failed Component Validation, due to the lack of the required Corrective Action Plan (CAP) that should provide detailed milestones which describe planned actions necessary for FFM to correct the security deficiency and remediate the weaknesses.

- **All FFM controls are described in CFACTS as "Not Satisfied".** Security controls are not documented as being fully implemented.

  This introduces the possibility that the FFM controls are ineffective. Ineffective controls do not appropriately protect the confidentiality, integrity and availability of data and present a risk to the CMS enterprise.

- NotResp

- **Control inheritance is incorrectly documented in CFACTS**. FFM indicates many of its controls are "under the control of the NotResp however, these controls are not marked as inherited from the NotResp and do not accurately describe the security control implementation within CFACTS. For example, many controls describe other systems such as the Rate and Benefit Information System (RBIS) and the Health Insurance Oversight System (HIOS).

Unclear control responsibility can lead to controls not being appropriately implemented and a lack of accountability.

- NotResp

Unclear role responsibility can affect the life cycle support of the FFM system.

Current Security Assessment Status Summary

Contractor	Assessment Status	POA&M (Y/N)
MITRE	*2 high, 22 moderate and 13 low findings remain open (4/12/2013) 11 moderate and 8 low findings remain open (9/19/2013	N

Points of Contact (POCs) were confirmed by CFACTS

System Level	Business Owner	Sys Developer/ Maintainer	ISSO
Moderate	James Kerr OA/CMHPO	Mark Oh OIS/CIISG/DHIM	Darrin Lyles OIS/CIISG/DSMDS

Documentation Artifacts

Authorization Request	SSP	RA	CP	CP Test	Security Assessment	PIA
	07/29/2013 redline version	Draft		none	*04/12/2013 08/30/2013 09/19.2013	Draft 2012

*There are weaknesses listed in CFACTS from a referenced document FFM_FFE_SCA_05032013-FFM_FFE-QHP_SCA. The weakness milestones were disapproved by EISG. The weaknesses were entered into CFACTS in May of 2013. There were additional security control assessment attempts in August and September 2013. ***The FFM could not be fully assessed.***