DEPARTMENT OF HEALTH & HUMAN SERVICES
Centers for Medicare & Medicaid Services
7500 Security Boulevard, Mail Stop N3-15-25
Baltimore, Maryland 21244-1850

OFFICE OF INFORMATION SERVICES

CENTERS FOR MEDICARE & MEDICAID SERVICES

MEMORANDUM

DATE:

TO: Director,
Consortium for Medicare Health Plans Operations (OA/CMHPO) and Acting Deputy Center Director for Operations, Center for Consumer Information and Insurance Oversight (CCIIO)

FROM: Chief Information Officer and
Director, Office of Information Services (OIS)

SUBJECT: Authorization Decision for the Federally Facilitated Marketplace (FFM) System

ACTION REQUIRED 30 DAYS FROM THE DATE OF THIS MEMORANDUM

The Federally Facilitated Marketplace (FFM) is a ***Moderate*** level system to be located at the Terremark datacenter in Culpeper, Virginia. The system maintains records used to support all Health Insurance Exchange Programs established by the Centers for Medicare & Medicaid Services (CMS) under the health care reform provisions of the Affordable Care Act (Public Law 11-148). FFM will help qualified individuals and small business employers shop for, select, and pay for high-quality, affordable health coverage. FFM will have the capability to determine eligibility for coverage, for tax credits, and for cost-sharing reductions; as well as eligibility for Medicaid, Basic Health Plan (BHP), and Children's Health Insurance Program (CHIP) coverage. As part of the eligibility and enrollment process, financial, demographic, and health information will flow through the Marketplace.

I am issuing an Authorization to Operate (ATO) for the FFM information system to operate in its current environment and configuration until **March 20, 2014**. The current configuration of FFM only includes: Qualified Health Plan (QHP); QHP-Dental; Eligibility & Enrollment (E&E) (except: Identify Proofing for Agent/Broker and Call Center initiated applications; Second chance application completion; Advance Premium Tax Credits (APTC) eligibility determination; Cost Sharing Reduction (CSR) eligibility determination; Outbound account transfer for eligibility determination; Change in circumstances for plan compare; Eligibility Support Desktop (ESD); Direct Enrollment issuer redirects for eligibility determination; Direct Enrollment minor web interface; Initial/Change Enrollment cancel/terminate functionality; Enrollment validation of parsing of inbound 834 messages; Enrollment outbound business acknowledgement generation; Enrollment State-Based Marketplace (SBM) inbound 834 transactions; Enrollment Data Store (EDS); Enrollment double dip check; Small Business Health Options Program; Call Center user interface; and Call Center notices and mailing); Financial Management (FM) (except: Vendor and banking collection information, SBM data collection, and CSR calculation); and Plan Management (PM) (except: QHP Public Use File, Unified Rate Review (URR) Content Reviewer, Plan ratification and accreditation, Plan transfer, Deficiency Notices, and LMI Analyzer).

This system is not authorized to establish any new connections or interfaces with non-CMS FISMA or other non-CMS connections without prior approval during the period of this ATO. An impact analysis must be conducted for any system changes implemented after the issuance of this ATO. Any major modifications that affect the security posture of the system will require an appropriately scoped security controls assessment and issuance of a new ATO.

The security authorization of the information system will remain in effect until the indicated expiration date if the following conditions are maintained:

(i) Required periodic security status reports for the system are submitted to this office in accordance with current CMS policy;
(ii) New vulnerabilities reported during the continuous monitoring process do not result in additional agency-level risk that is deemed unacceptable; and
(iii) The system has not exceeded the maximum allowable time between security authorizations in accordance with Federal or CMS policy.

The attachment provides information on requirements not met, as well as corrective actions needed to bring them into compliance. The actions set forth in the attachment must be entered into the approved CMS Plan of Action and Milestones (POA&M) tracking tool no later than 30 days from the date of this memorandum, and the action items addressed no later than the designated completion dates. This office will monitor all POA&M items submitted during the period of authorization.

If you have questions, please contact Teresa Fryer, Chief Information Security Officer (CISO), at 410-786-2614. The DISPC team is also available to support staff level questions at CISO@cms.hhs.gov.

Tony Trenkle

Attachment

cc:
Mark Oh, Director OIS/CIISG/DHIM
Darrin Lyles, ISSO, OIS/CIISG/DSMDS
Teresa Fryer, CISO, Director OIS/EISG
Michael Mellor, Dep. CISO, Dep. Director OIS/EISG
Desmond Young, OIS/EISG/DISPC
Jessica Hoffman, OIS/EISG/DISPC
James Mensah, OIS/EISG/DISPC

Attachment

Federally Facilitated Marketplace (FFM) System

Authorization Decision

Authorization decision is required for the following reason(s):

	New System
X	Major system modification
	Serious security violation
	Changes in the threat environment
	Expired authorization to operate

I. Authorization Decision

X	**Authorization to Operate** The applicable system is authorized to operate until the designated date, subject to the authorization actions in Section II.

This authorization will expire: March 20, 2014. This authorization may be withdrawn at the discretion of the Authorizing Official for lack of progress on the authorization actions in Section II, or any security violations deemed to increase the risk to CMS beyond a tolerable level.

	Denial of Authorization to Operate The applicable system may not operate until the authorization actions listed in Section II are completed, after which, verification of corrective actions and resubmission of the authorization package is required.

_____
(Authorizing Official Signature and Date)
Tony Trenkle
CMS Chief Information Officer

Federally Facilitated Marketplace (FFM) System

II. Authorization Actions

Failure to meet the assigned due dates without prior approval invalidates this authorization to operate. The following specific actions are to be completed by the date(s) indicated:

Finding	Finding Description	Recommended Corrective Action	Risk	Due Date
NotResp	NotResp		NotResp	July 31, 2015
END OF ACTIONS				

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.***