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: SEP 3 2013

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 Federal Facilitated Marketplaces (FFM) System

ACTION REQUIRED 30 DAYS FROM THE DATE OF THIS MEMORANDUM

The Federal Facilitated Marketplaces (FFM) System is a ***Moderate*** level system 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. Exchanges will have the capability to determine eligibility for coverage through the Exchange, for tax credits and cost-sharing reductions, and 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 (potentially) health information will flow through the Exchange.

On August 8, 2013, you certified the controls for the system and submitted along with your certification the other required documentation necessary to obtain an Authorization to Operate (ATO) for FFM.

I have determined through a thorough review of the authorization package that the risk to CMS information and information systems resulting from the operation of the FFM information system is acceptable predicated on the completion of the actions described in the attachment. Accordingly, **I am issuing an Authorization to Operate (ATO)** for the FFM information system to operate in its current environment and configuration until **August 31, 2014**. The current configuration includes only the Federal Facilitated Marketplaces Qualified Health Plans (QHP) and Dental modules. 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 [redacted]. The DISPC team is also available to support staff level questions at [redacted]@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 Marketplaces (FFM) System

Authorization Decision

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

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

I. Authorization Decision

I have reviewed the information concerning the request for an Authorization to Operate and with consideration of the recommendations provided by my staff; I concur with the assessment of the security risk. This risk has been weighed against the business operational requirements and security measures that have or will be implemented. I have determined the following authorization decision is appropriate.

X	**Authorization to Operate** The current risk is deemed acceptable. The applicable system is authorized to operate until the designated date, subject to the authorization actions in Section II.
This authorization will expire: August 31, 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 current risk is deemed unacceptable. 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

Attachment

Federally Facilitated Marketplaces (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
FFM has an open high finding: [redacted]	[redacted] the threat and risk potential is limitless. [redacted]	[redacted]	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. (CA-2).	May 31, 2014

Attachment

Federally Facilitated Marketplaces (FFM) System

Finding	Finding Description	Recommended Corrective Action	Risk	Due Date
FFM has an open high finding: [redacted]	[redacted]	[redacted]	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. (CA-2).	February 26, 2015

Attachment

Federally Facilitated Marketplaces (FFM) System

Finding	Finding Description	Recommended Corrective Action	Risk	Due Date
[redacted]	[redacted] Security controls are not documented as being fully implemented.	[redacted]	There is the possibility that the FFM security controls are ineffective. Ineffective controls do not appropriately protect the confidentiality, integrity and availability of data and present a risk to the CMS enterprise. (PL-2).	February 7, 2014
[redacted]	[redacted]	[redacted]	[redacted] exposes the enterprise to additional risk. (RA-2).	February 7, 2014
[redacted]	[redacted]	Review the FIPS 199 inheritance selections in CFACTS and either select the appropriate inheritance or indicate the controls are solely the responsibility of FFM.	[redacted] can lead to controls not being appropriately implemented and a lack of accountability. [redacted]	February 7, 2014

Attachment

Federally Facilitated Marketplaces (FFM) System

Finding	Finding Description	Recommended Corrective Action	Risk	Due Date
Inconsistent Points of Contact (POCs).	The system developer/maintainer on the CMS Security Certification Form is a different person from [redacted]	Identify and update the appropriate system POCs for all of the documents and provide the updated POCs [redacted]	Unclear role responsibility can affect the life cycle support of the system. [redacted]	February 7, 2014
END OF ACTIONS				