**DATE:**

**TO:** Marilyn Tavenner

**FROM:** James Kerr, Consortium Administrator for Medicare Health Plans Operations
Henry Chao, Deputy Chief Information Officer & Office of Information Services Deputy Director

**SUBJECT:** Federally Facilitated Marketplace–DECISION

**ISSUE:**

The Federal Information Security Management Act (FISMA) requires that the various Federally Facilitated Marketplace (FFM) systems - Enterprise and Eligibility (E&E), Financial Management (FM), and Plan Management (PM) successfully undergo a Security Control Assessment (SCA). Due to system readiness issues, the SCA was only partly completed. This constitutes a risk that must be accepted and mitigated to support the Marketplace Day 1 operations.

**BACKGROUND:**

CMS utilizes independent and specialized contractors to test the security readiness of its systems. Testing of the Marketplace has been on-going since inception as part of the CMS Expedited Life-Cycle process with the latest security testing occurring in September of 2013. As with all new systems which are pending launch, there are inherent security risks with not having all code tested in a single environment, finally, the system requires rapid development and release of hot-fixes and patches so it is not always available or stable during the duration of testing,

From a security perspective, the aspects of the system that were not tested due to the ongoing development, exposed a level of uncertainty that can be deemed as a high risk for FFM. Although throughout the three rounds of SCA testing all of the security controls have been tested on different versions of the system, the security contractor has not been able to test all of the security controls in one complete version of the system.

The risk associated with issuing an ATO for the FFM will be reduced by instituting a two-part mitigation plan.

First, CMS will implement the following security processes for the first year of operation of FFM:

- Establish a dedicated security team under the Chief Information Officer (CIO) to monitor, track and ensure the mitigation plan activities are completed. The CIO and the Chief Information Security Officer (CISO) will report weekly on the progress to the Health Reform Operations Board;

- Monitor and perform weekly testing of all border devices, including internet facing web servers;
- Conduct daily/weekly scans using the CISO's continuous monitoring tools
- Conduct a full SCA test on FFM (E&E, FM and PM) in a stable environment where all security controls can be tested within 60/90 days of going live on October 1st.

Second, CMS will migrate the Marketplace systems to CMS' Virtual Data Center (VDC) environment in Q1-2014. This environment has been through a full security assessment and has an authority to operate.

**RECOMMENDATION:**

Issue an Authority-to-Operate (ATO) for six months and implement the mitigation plan. The six-month period will allow the Marketplace to normalize its development activities while enabling the security team to closely monitor activities and perform a complete SCA.

**DECISION:**

Approve [redacted] Date SEP 27 2013

Disapproved_____ Date_____

*Marilyn Tavenner*

Attachment: Federally Facilitated Marketplace Decision Memo Risk Acknowledgment Signature Page

DEPARTMENT OF HEALTH & HUMAN SERVICES
Centers for Medicare & Medicaid Services

[redacted]

**Federally Facilitated Marketplace Decision Memo**
**Risk Acknowledgment Signature Page**

We acknowledge the level of risk the Agency is accepting in the Federally Facilitated Marketplace (FFM). The mitigation plan does not reduce the risk to the FFM system itself going into operation on October 1, 2013. However, the added protections do reduce the risk to the overall Marketplace operations and will ensure that the FFM system is completely tested within the next 6 months.

Reviewer [redacted] Date 9-27-2013
Teresa Fryer

Reviewer [redacted] Date 9-27-2013
Tony Trenkle

Reviewer [redacted] Date 9-27-2013
Michelle Snyder