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: Macros enabled on uploaded files allow code to execute automatically.	An excel file with a macro which executes when the spreadsheet is opened was uploaded for review by another user. The macro only opened up a command prompt window on the local user's machine; however, the threat and risk potential is limitless. Keeping macros enabled relies on the local machine of the user who downloads to detect and stop malicious activity.	Implement a method for scanning uploaded documents for malicious macros. Ensure that the existing or equivalent compensating controls remain in place: • The file upload function is only available for a limited period each year. • The file upload function is not available to all users, only plan users. • Files types able to be uploaded are whitelisted.	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