The FFM application has a "Moderate" Federal Information Processing Standard (FIPS) impact level since it contains PII information. Any system rated with a "Moderate" impact must ensure that it implements security controls that will protect information thoroughly and effectively within the system. Most of the findings in this document can fall into the following areas:

- **Access Control:** Security access rights to data need to be tightened.
- **Parameter Validation:** There were a couple of findings that pertained to proper parsing of input parameters.

1.4 Summary of Recommendations

For each finding, Blue Canopy has developed detailed recommendations for improvements that address the findings and the business risk, as well as strengthen CMS information security. While all findings will need to be addressed, findings representing a high risk to CMS data should be addressed first and closed or mitigating controls implemented to reduce the risk exposure to CMS. Most of the recommendations in this document can fall into the following areas:

Parameter Validation: The NotResp parsing engine did not properly handle specially crafted messages that were designed to consume memory. As a result, consumption of these NotResp messages would cause he service to crash. The recommendation is to perform additional filtering on the service before parsing the NotResp message.

Publically Accessible Data: Using 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.