DEPARTMENT OF HEALTH & HUMAN SERVICES
Centers for Medicare & Medicaid Services
7500 Security Boulevard, Mail Stop N2-14-26
Baltimore, MD 21244-1850

CENTERS FOR MEDICARE & MEDICAID SERVICES

Office of Information Services
7500 Security Boulevard
Baltimore, MD 21244-1850

Health Insurance eXchange (HIX) August – September 2013 Security Control Assessment (SCA) Report

Final Report

October 11, 2013

Table of Contents

List of Tables

List of Figures

1 EXECUTIVE SUMMARY

The Centers for Medicare & Medicaid Services (CMS) of the United States Department of Health and Human Services (HHS) engaged The MITRE Corporation (MITRE) to perform an onsite application-only security control assessment (SCA) of the Health Insurance eXchange (HIX) modules that were not tested previously. Specifically, the Plan Management (PM), Financial Management (FM) and the Enrollment and Eligibility (E&E) modules as part of the CMS Certification and Accreditation (C&A) Program. MITRE conducted (1) an audit to ensure that the application complied with CMS security instructions, (2) a configuration audit to determine if security controls were implemented correctly, (3) a technical infrastructure test where applicable, (4) interviews, and (5) documentation reviews to determine if security controls were implemented correctly.

Since the construction of the infrastructure for the servers which began in 2012, the Health Insurance eXchange (HIX) has been referenced a variety of ways in documentation, speech, and systems of records. Below is a list of terms used to reference the HIX system. This document may use these terms synonymously:

- Health Insurance eXchange (HIX)
- Health Information eXchange – (HIX) incorrectly
- Federally Facilitated Marketplace (FFM) – or "Marketplace"
- Federally Facilitated Exchange (FFE) or "Exchange"

1.1 HIX BACKGROUND

A key provision of the Affordable Care Act (ACA) is the implementation of Insurance Marketplaces (Marketplaces). The Center for Consumer Information and Insurance Oversight (CCIIO) is responsible for providing guidance and oversight for the Marketplaces. A Marketplace is organized to help consumers and small businesses buy health insurance in a way that permits easy comparison of available plan options based on price, benefits and services, and quality. The ACA provides each State with the following options:

- Set up a State-Based Marketplace (SBM)
- Designate a non-profit entity to operate a State-Based Marketplace
- Collaborate with another state or a consortium to operate a Marketplace
- Defer to the Federally Facilitated Marketplace

The Marketplaces will carry out a number of functions required by the ACA, including certifying Qualified Health Plans (QHPs), administering Advance Premium Tax Credits (APTCs) and Cost Sharing Reductions (CSRs), and providing an easy-to-use website so that individuals can determine eligibility and enroll in health coverage. The Marketplaces will therefore be required to interact with a variety of stakeholders, including consumers, navigators, agents, brokers, employers, Health Plan Issuers, State-based Medicaid and Children's Health Insurance Programs (CHIPs), Federal agencies for verification checks, third-party data sources, and State Insurance Departments.

The HIX is comprised of several applications, commonly referred to as modules or business areas. Descriptions of these modules are listed below:

1.1.1 Plan Management (PM)

The Plan Management (PM) business area consists of business processes for acquiring, certifying, monitoring, renewing, and managing the withdrawal of qualified health plans (QHPs) and the Issuers that offer these plans for a given Marketplace. These areas are currently supported by a composite solution consisting of:

- Data submission templates (MS Excel-based) allowing States and Issuers or their representatives to download, populate, validate, and upload into the PM system various complex data sets detailing application, plan, and rate and benefits information.
- User interfaces and services for State and Issuer users to submit, review, modify, and attest to the information uploaded or provided directly via the user interface to support the application and rate and benefits collection process for a given marketplace or set of marketplaces.
- User interfaces and services for CMS personnel to review, monitor, and certify/decertify applications and plans submitted for approval in a given marketplace.
- System interfaces to existing CMS systems (e.g., Health Insurance Oversight System [HIOS]) to support streamlined data and profile collection and authentication.
- A system interface to CMS' portable document format (PDF) generation solution, (b)(5), (b)(6), (b)(7)c, (b)(7)e to create notices that are distributed to Issuers.

The PM application design is supported by a scalable, 3-tiered environment running on the CMS (b)(5), (b)(6), (b)(7)c, (b)(7)e database. The user interface design is based on the CMS.gov web brand including Healthcare.gov, CMS.gov, and Medicare.gov. It is Section 508 compliant and uses a Progressive Enhancement approach.

The Resubmission functionality provides the ability for Issuers to resubmit a plan for any of the following reasons:

- To address an application deficiency noted by HHS or the State
- To submit a data correction during the plan preview period
- To submit additional information for certification of stand-alone dental plans.

By initiating resubmission, the Issuer is temporarily invalidating the previously submitted QHP so that information related to one of the aforementioned factors above can be modified and resubmitted. Only QHPs with a *Cross Validation Completed* status may be resubmitted. Initiating resubmission for any module will change that module status to *Pending Submission* and all other modules to *Validation Completed.*

There is a Plan Preview ability that provides Issuers with the capability to view rates and plan details based on a set of subscriber and plan variance data selected by the user. The Summary page provides the user with the ability to select a specific IssuerID to preview their plan(s). The user can view an Issuer's submitted plans and rating scenarios by clicking on the View Plans button that corresponds to an Issuer in the Issuer table. The Rating Scenarios page allows the user to select plans and various inputs necessary for the rating engine to provide a rate(s).

The CMS Certification/Suppression module page serves two functions to CMS users. First, it provides CMS users with a daily report of all QHPs submitted to FFM, along with chief executive officer (CEO) contact information associated with each plan. The daily report includes all QHPs in the Marketplace and plans submitted through the National Association of Insurance Commissioners (NAIC) System for Electronic Rate and Form Filing (SERFF) and loaded into the Marketplace with a *Cross Validation Completed* status. Second, it provides CMS users the ability to set or change the status of a plan. CMS also uses this page to make any suppression changes to the plan. CMS users must select search criteria, using either IssuerID or PlanID, and click Search to display the results. The CMS user can then suppress a plan or cancel a plan suppression while adding or altering a suppression reason code.

1.1.2 Eligibility & Enrollment (E&E)

The Eligibility and Enrollment (E&E) module comprises services that are necessary to verify an applicant's eligibility for health insurance, plan selection and enrollment through the Marketplace. Eligibility determination includes, but is not limited to: income verification, citizenship verification, lawful presence verification, incarceration status verification, and verification of eligibility for other public minimum essential coverage or employer-sponsored minimum essential coverage health plans.

As applicants go through the steps to apply for insurance in the Marketplace, the applicants are prompted as to whether they qualify for a QHP, APTCs, CSRs, or other insurance such as State-based Medicaid or CHIP. Upon completion, health insurance benefits available to the applicant (and household members, if applicable) are displayed. Then the applicant can decide upon the insurance coverage that suits the household's needs, based on the information populated and verified in the Application.

Federal Tax Information (FTI) is collected in E&E and is stored in a (b)(5), (b)(6), (b)(7)c, (b)(7)e instance that is logically separated (b)(5), (b)(6), (b)(7)c, (b)(7)e The FFM three-tiered architecture includes a Presentation Zone, an Application Zone, and a Data Zone. The user interface (UI) is located in the Presentation Zone, while FTI is located in the Data Zone, with the Application Zone in between. The user interface (UI) does not directly access FTI. The UI goes through the Application Zone to request FTI.

E&E has several distinct functions that are described below.

1.1.2.1 My Account

My Account is available to consumers (Public applicants or their designees). Specifically, consumers will be able to create a National Institute of Standards and Technology (NIST) Level of Assurance 2 (LOA2) account in the Marketplace, log in to the Marketplace using that LOA2 account, and perform maintenance activities on their account (e.g., update email address and reset password). The My Account page allows a Marketplace user to monitor and change all information related to the user's eligibility for an affordable insurance program. After a user registers and logs in, the user can update settings, grant other users access to their health insurance application (Application), review selection history, and report changes in circumstance.

1.1.2.2 Individual Application

The Individual Application captures the necessary information for the Marketplace to verify an applicant's eligibility for enrollment in a QHP. The applicant answers questions for citizenship status or lawful presence, residency information, and incarceration status to determine the applicant's eligibility to enroll in an affordable insurance plan. If a user requests financial assistance, the applicant answers additional questions to see if the applicant might be eligible for APTCs, CHIP, Medicaid, or CSR. Applicant-entered information triggers what web pages the applicant must complete to determine eligibility.

1.1.2.3 Plan Compare

When a user is ready to look at insurance plans the user accesses the Plan Compare pages. Plan Compare allows the user to view eligible plans and compare and view plan details. The user can customize and filter the plans displayed by selecting relevant criteria. For example, the user can filter by plan type, premium amount, maximum out-of-pocket expenses, deductible, CSR-eligible plans, metal level, and insurance company. Users can sort the results by premium and maximum out-of-pocket expenses. When users are ready to select a plan, they can add it to their cart from any page.

1.1.2.4 Eligibility Support Desktop

The Eligibility Support Desktop (ESD) provides the Eligibility Support Staff (ESS) members the ability to review the evidence documents provided by the consumer to resolve an inconsistency. The ESS worker can adjudicate the resolution of inconsistencies based on the authorized evidence documents delivered. As each evidence document is loaded into the ESD, a task is generated on the appropriate ESS member's Home page.

The task queue on the home page provides a list of all tasks that have been assigned to the ESS member based on the credentials entered; each ESS member is assigned a specific type of inconsistency or work type to review. Once the ESS member selects a task from the task queue, the ESD directs the worker to the Overall Records View page for the ESS member to start the review process on the Application with the inconsistency.

The Overall Record View page provides a high-level overview to the ESS worker of the Application's inconsistency and the relationship to the Applicant in terms of coverage, eligibility determinations, and pending inconsistencies. During the review and adjudication process, the ESS member can change the status of a document to sufficient or insufficient. The Applicant's Application status is updated to *Pending Additional Documentation*. During the review process, the ESS worker can reference the attested information during the individual or paper Application process.

1.1.2.5 Call Center Integration

The Next Generation Desktop (NGD) accesses FFM to retrieve basic history and information about the user's account, eligibility and enrollment history. FFM will expose the Call Center Representative (CCR) services directly to the Call Center application (b)(5), (b)(6), (b)(7)c, (b)(7)e the Application Zone and bypasses the Hub. For certain services, the CCRs use the same UI that the individuals use to assist a caller complete the Application eligibility and enrollment processes. Any update transactions go through the FFM UI.

1.1.2.6 Direct Enrollment

Consumers shopping for health insurance for themselves and/or their household members have the choice of enrolling in a QHP by accessing the FFM website directly, or by shopping via a partner website. The Direct Enrollment application programming interface (API) services facilitate integration between partner websites and FFM to support consumers shopping/enrolling in QHPs through partner websites.

FFM supports two models for partner websites to integrate their consumer shopping experience with FFM:

- Direct Enrollment API: Under this model, partner websites use FFM' User Interface services and Web services to implement a consumer's eligibility determination and plan shopping functions.
- Lead Generation API: Under this model, partner websites provide educational content and pre-sell their plans before transferring the consumer to the FFM website. The consumer completes all functions including eligibility determination, plan shopping and enrollment on FFM. However, the partner website specifies Issuer/Plan filters that FFM applies as part of the consumer's plan shopping. This model is offered as an alternative to the Direct Enrollment API to support Issuers that may not be ready to implement the full Direct Enrollment API.

Federal Functions (Double Dipping)

Double Dipping includes verifying that an individual does not receive APTC/CSR from both a SBM and FFM. This process includes a check with the Enrollment Data Store (EDS) to determine if an individual is enrolled in a SBM and, if so, if they are already receiving ATPC/CSR through a SBM. If the individual is already receiving APTC/CSR, this process denies an individual APTC/CSR eligibility within FFM and prevents an individual from applying APTC/CSR in Plan Compare.

Federal Functions (EDS to store FFM and SBM Transactions)

FFM and SBM enrollment data sent to FFM will be stored in the Federal Exchange Program Systems (FEPS) EDS for the purpose of enabling Federal payments of APTC or CSR, and preventing duplicate APTCs across multiple Marketplaces. FFM will send a transaction to the issuer and a copy to the EDS directly. In the case of SBM, the Hub will facilitate the exchange of 834 transactions between parties. Specifically, the Hub will serve as the gateway for enrollment transactions between the SBM and EDS, accepting copies of enrollment transactions sent by SBMs to QHP issuers that offer coverage through SBMs.

1.1.2.7 Enrollment

Consumers can compare Plans, select a Plan, and enroll under a QHP. The enrollment information is sent to the Issuer for servicing. An enrollment is effectuated only after the consumer pays the first monthly premium to the Issuer. The consumer has the option to pay the first monthly premium as part of the enrollment process by being redirected to the Issuer's payment portal. All new enrollments will be sent to Issuers using X12 834 EDI transactions. Issuers will respond to FFM, also using the X12 834, with information on effectuation of the enrollment. If the first monthly premium is not received on time, the effectuation date may be moved back to the next applicable month.

1.1.2.8 Notices

The Notices for the Marketplace provide paper and electronic communication to the individual consumer. All Notices generated by the Marketplace are addressed and sent to the person designated to receive official communications, and are sent according to the communication preferences set by this person within My Account. A Notice is always sent in electronic format to the consumer's Bulletin Board and would also be printed and mailed if US Mail had been selected as a communications preference. When a Notice is sent electronically, an email or text message notification is sent to the contact person as well, informing them that there is official communication from the Marketplace waiting for them to review.

The following notices are scheduled for Day One:

- Eligibility Determination Notice
- ESD Custom Notice Template
- Data Sources Down Notice
- Remote Identity Proofing (RIDP) Failure Notice
- Request for More Info – Income
- Request for More Info – Step 3, 4 Immigration Status Notice

1.1.2.9 Mailing Contractor Integration

The Marketplace Mail Contractor Integration is responsible for transferring Notices flagged during the day for delivery by US Mail over to the mail contractor on a daily basis for printing. A batch process will retrieve the files to be sent and place them within a zip for transfer; there can be one or more zip files sent daily as there will be a maximum number of notice files that can be zipped into one. The Mail Contractor is responsible for printing and mailing the Notices and returning a response file to the Marketplace; this response file includes the confirmation of receipt and print date of each Notice file. The Marketplace stores the results received from the mail contractor.

1.1.3 Financial Management (FM)

Two Financial Management (FM) components are being implemented. They are:

- State Based Marketplace (SBM) Data Collection and Validation
- Preliminary and Final CSR Calculation

To support oversight and federal functions, SBMs are required to submit a subset of rate and benefit data for certified QHPs to FEPS via Enterprise File Transfer (EFT). For SBMs that use SERFF, data is extracted from SERFF. SBMs that do not use SERFF are required to extract the required data in the prescribed format described SBM Interface Control Document (ICD). All file submissions are full replacement files; all data elements should be sent with each submission.

Files are subjected to an initial file validation as well as data validations similar to those performed during the data collection in the FFM Plan Management templates. As part of the data intake process, the system obtains the EHB Portion of Allowed Claims, PM amount from the Unified Rate Review database based on the submitted Plan ID. Records that pass data validation are stored for future processes. Records that fail data validation are rejected. At the conclusion of the data validation process, an error report detailing failed data validations is sent to the SERFF/SBMs via EFT so data can be corrected and resubmitted as required. CMS has the ability to approve or disapprove the accepted records.

The submitted certified plan information is used to support future federal functions, including the calculation of advance CSR amounts and Edge Server processes.

The Advance CSR Payment Estimate process allows CMS to calculate and evaluate advance CSR payment amounts based on information submitted by Healthcare Marketplaces. At designated intervals, authorized CMS/CCIIO users will initiate the process to calculate advance CSR payment amounts within the FEPS.

Once the Advance CSR Payment Estimate process completes, CSV files containing the data required for outlier analysis are generated for rate analysis. Authorized users will review the results and have the ability to manually correct the calculations. The final amounts will undergo a review and approval process. Approved calculations will be submitted to Issuers and States via (b)(5), (b)(6), (b)(7)c, (b)(7)e ia EFT.

1.2 Assessment Scope

To determine the potential security risks to CMS, MITRE was tasked with providing an application-only SCA of the HIX updates and HIX modules that were not tested previously (e.g.PM, FM, and E&E modules). The physical location of the servers hosting the applications and databases is at th (b)(5), (b)(6), (b)(7)c, (b)(7)e The assessment took place at the CGI Federal building located in Herndon, Va. The application was assessed August 19-30, 2013 and additionally September 16-19, 2013. Two separate test plans were drafted and submitted, one for each assessment. For the assessment in August 2013, please reference "*HIX August 2013 SCA FINAL_Test_Plan-08 21 2013.doc*". The September test is referenced as "*HIX-A September 2013 SCA Final_Test_Plan-09 17 2013.doc*". MITRE only considered the "as-is" application and did not consider future enhancements. MITRE performed the following activities during the multiple assessments:

- Interviewed selected personnel
- Reviewed system baselines
- Performed application security testing
- Reviewed database configuration settings
- Reviewed operating system settings for findings remediation of prior assessments
    - QHP in March through April of 2013

  - QHP-Dental Plans – June 2013
- Reviewed supplied security documentation

1.2.1 Joint Assessments

The August and September assessments were joint assessments with other companies (Booz Allen Hamilton, Blue Canopy and Deloitte), the Data Services Hub (DSH) and the Internal Revenue Service (IRS).

1.2.1.1 August 2013

The August 2013 assessment of HIX was run in parallel with the Data Services Hub (DSH) assessment. Joint meetings and daily out briefs were performed. Shared information and ad-hoc meetings with HIX and DSH groups were necessary to understand the integrations between the two systems.

IRS and Booz Allen Hamilton (BAH) representatives were onsite during the DSH and FFM assessments to investigate FTI usage in the DSH and HIX systems. The funding of BAH and the IRS efforts were not provided under by MITRE's SCA contract. An instance of the HIX (b)(5), (b)(6), (b)(7)c, (b)(7)e assessed because of changes made since June 2013 to accommodate FTI. DSH and HIX provided documentation, SCA scans, questionnaires, demos, and findings which were provided to the IRS and BAH at the request of CMS/CCIIO. IRS and BAH findings, reports and artifacts were not shared with MITRE and will not be reflected in this report. More information about IRS and BAH interactions can be found in the August 2013 test plan and daily out brief agendas.

1.2.1.2 September 2013

The September 2013 assessment of HIX was a joint assessment between MITRE and Blue Canopy/Deloitte for staff augmentation and contract transition efforts. Funding of Blue Canopy and Deloitte personnel was not provided by MITRE's SCA contract. Blue Canopy is the new SCA contractor as the Q2 2013 awarding of the SCA contract. Both groups collaborated with equal access to the HIX documentation, scans, interviews and past HIX assessments as directed by CMS/CCIIO. The application testing was divided between MITRE and Blue Canopy with separate reports being provided by both.

The following CMS Acceptable Risks Safeguards/CMS Minimum Security Requirements (ARS/CMSR) security control families were the focus for the HIX PM, FM, and E&E modules assessment:

- Access Control (AC), all controls except AC-1, AC-18, AC-19, and AC-20
- Awareness and Training (AT), only AT-2 and AT-3
- Audit and Accountability (AU), all controls except AU-1
- Security Assessment and Authorization (CA), all controls except CA-1
- Configuration Management (CM), all controls except CM-1
- Contingency Planning (CP), all controls except CP-1, CP-6, CP-7, CP-8, and CP-9
- Identification and Authentication (IA), all controls except IA-1 and IA-3

- Maintenance (MA), only MA-3
- Media Protection (MP), only MP-5 and MP-6
- Physical and Environmental Protection (PE), only PE-2, PE-5, and PE-17
- Planning (PL), all controls except PL-1 and PL-4
- Personnel Security (PS), all controls except PS-1, PS-2, PS-3, and PS-8
- Risk Assessment (RA), only RA-2 and RA-3
- System and Services Acquisition (SA), all controls except SA-1, SA-7, and SA-9
- System Communications (SC), all controls except SC-1, SC-4, SC-12, SC-17, SC-20, SC-21, SC-22, and SC-32
- System and Information Integrity (SI), all controls except SI-1, SI-3, SI-5, and SI-8

This application-only SCA is one portion of an overall Information Security Program to help management determine the security risks this application presents to CMS. This report contains the results of that effort.

1.3 Known Functionality Not Tested

Below is a list of functionality MITRE was made aware of but was deemed out of scope by CMS for various reasons. This may not be a comprehensive list of functionality that has not been tested in the E&E, PM and FM modules since a comprehensive list of functionality per module has never provided to MITRE.

- Out of Scope for August 2013 Assessment
  - PM : Plan Ratification, Certification, and Accreditation
  - PM : Plan Transfer
  - PM : Deficiency Notices ((b)(5), (b)(6), (b)(7)c, (b)(7)e anticipated 9/23/2013)
  - PM : LMI & MIDAS Extras (postponed until LMI Analyzer SCA anticipated 10/15/2013)
- Out of Scope for September 2013 Assessment
  - E&E –Eligibility Support Desktop (ESD)
  - E&E – Call Center
  - FM: SBM Data Collection – User Interface
  - FM: CSR Calculation– User Interface

Below is a list of functionality that was in scope for this assessment but MITRE was not able to test.

- E&E – Direct Enrollment, Issuer redirects consumer to FFM to complete application & determine eligibility functionality.
- E&E – Enrollment, Initial Enrollment and Change Enrollment (Cancel / Terminate) functionality.
- E&E – Notices & Mailing

1.4 Summary of Assessment

The August and September 2013 assessments of the HIX did not assess functionally complete versions of the Eligibility & Enrollment (E&E), Financial Management (FM), and Plan Management (PM) modules in the same environments. Documentation provided divulged some known functional limitations and omissions due to the software still being developed. The provided lists omitted numerous issues that required investigation to resolve. Workarounds to the components being tested were provided that impacted end to end MITRE test cases.

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 focused 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.

- **Testing environments and module interconnections were not ready for the SCA**. Specifically during the September assessment, MITRE was given three different environments to test in (b)(5), (b)(6), (b)(7)c, (b)(7)e t various times to over the course of the assessment to compensate for lack of interconnections between modules. These environments were not vetted or tested by CMS or the development contractor prior to the onsite assessment to ensure the HIX workflows were functional. Test data manually entered by MITRE, in most instances, was unable to be validated as needed by the workflow to allow testing to proceed to the next step in the HIX Workflows.
- **Valid test data was not provided prior to testing**. MITRE requested that test data be pre-populated in the HIX application's database prior to the onsite so testers could start testing anywhere within the workflow of the application. This pre-populated data was never provided. In a three step process (1. Account Creation, 2. Individual Application creation, and 3. Plan Compare) MITRE had to create an Account and Application every time to run one test case for Plan Compare testing. Each test case took approximately 45 minutes to an hour to set up. Specifically, for an Application for a family of four, there is over 400 data elements (name, address, SSN, etc.) that need to be entered in the Individual Application. There are also system validations and calls to other applications (SSN validation) that need to be performed.
- **Test environment availability was not consistent**. Several times during the SCA the testing environments "went down" due to DSH, EIDM or HIOS systems being taken off line or rebooted. These events would occur without warning and only after the systems were taken off line was MITRE informed. This caused many outages and black out windows for SCA testing because the system was functionally unusable.
- **Environments were not dedicated to SCA testing.** It was reported that other groups were working in the provided testing environment. CMS instructed MITRE that SCA efforts to interrupt the availability of the system, such as attempting (b)(5), (b)(6), (b)(7)c, (b)(7)e exploits, were not to be performed. Due to this limitation MITRE was unable to determine the ability of HIX to withstand such attacks by a malicious user.

1.5 Summary of Findings

Findings for the HIX application have previously been reported to CMS for the QHP assessment March/April 2013 and QHP-Dental functionality June 2013 in separate reports. Those findings have been entered into CFACTS under the name "HIX". The findings below will be reported to CMS and CFACTS under the name "FFM" as directed by CMS/CCIIO. For a total sum of detailed findings for the HIX System, reference "HIX" and "FFM" in CFACTS.

The below summary only contains MITRE's findings for the August and September 2013 assessments of the HIX application. Contact Blue Canopy and Deloitte for further details on their findings.

Of the 28 findings discovered by MITRE in this assessment, 2 were considered High risks, 17 Moderate risks, and 9 Low risks. The risks found during the assessment are broken down as shown on the chart in Figure 1.

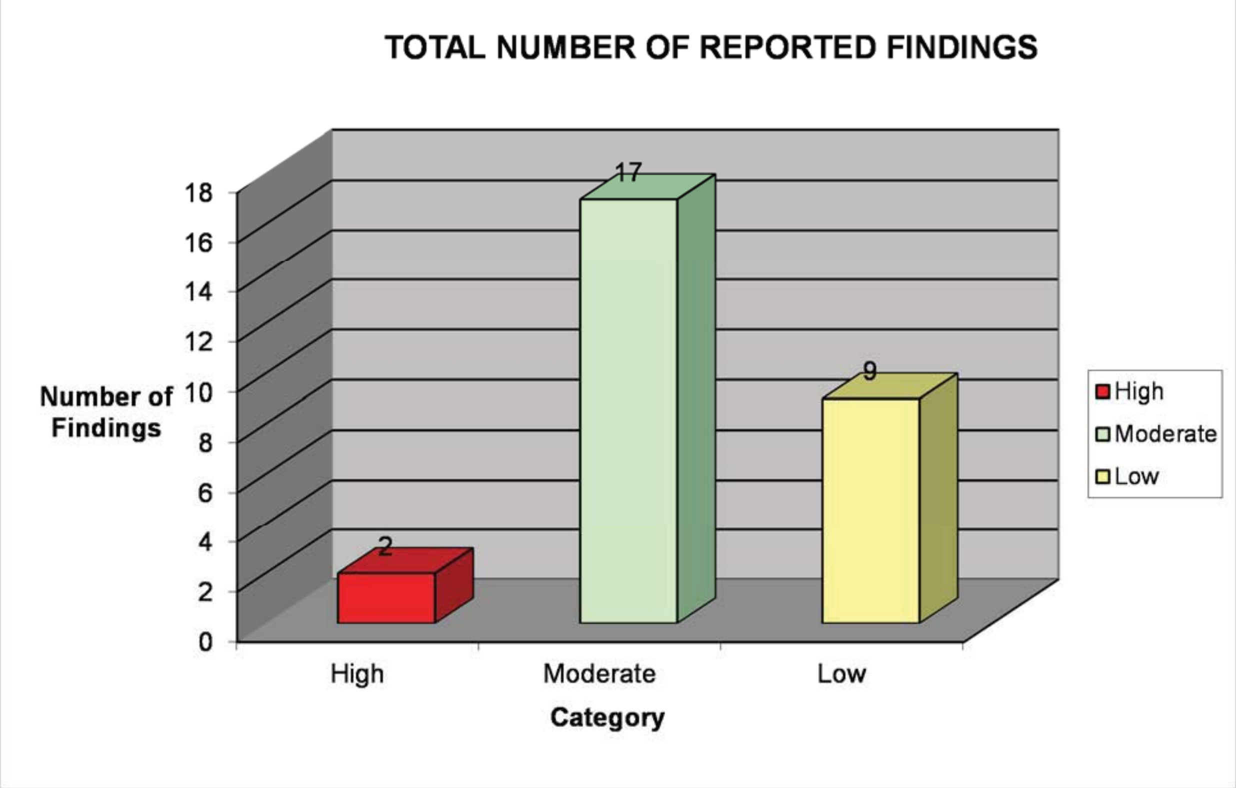

Figure 1. Reported Findings by Risk Level

As a result of efforts to remediate findings, of the 28 initial findings discovered in the system, no High risk findings, 11 Moderate risk findings and 8 Low risk findings remain open from this assessment and will be assigned to the HIX application. One HIGH finding was identified in the (b)(5), (b)(6), (b)(7)c, (b)(7)e a fix was retested and accepted to close the finding (b)(5), (b)(6), (b)(7)c, (b)(7)e environment. It is assumed that this fix will be deployed to (b)(5), (b)(6), (b)(7)c, (b)(7)e code drop. Six previously identified risks (5 Moderate and 1 low) were reassigned to other systems, and were marked "informational". These six risks are no long the responsibility of the HIX application, see section 3.4 for more information. The remaining open risks found during the assessment are broken down as shown on the graph in Figure 2.

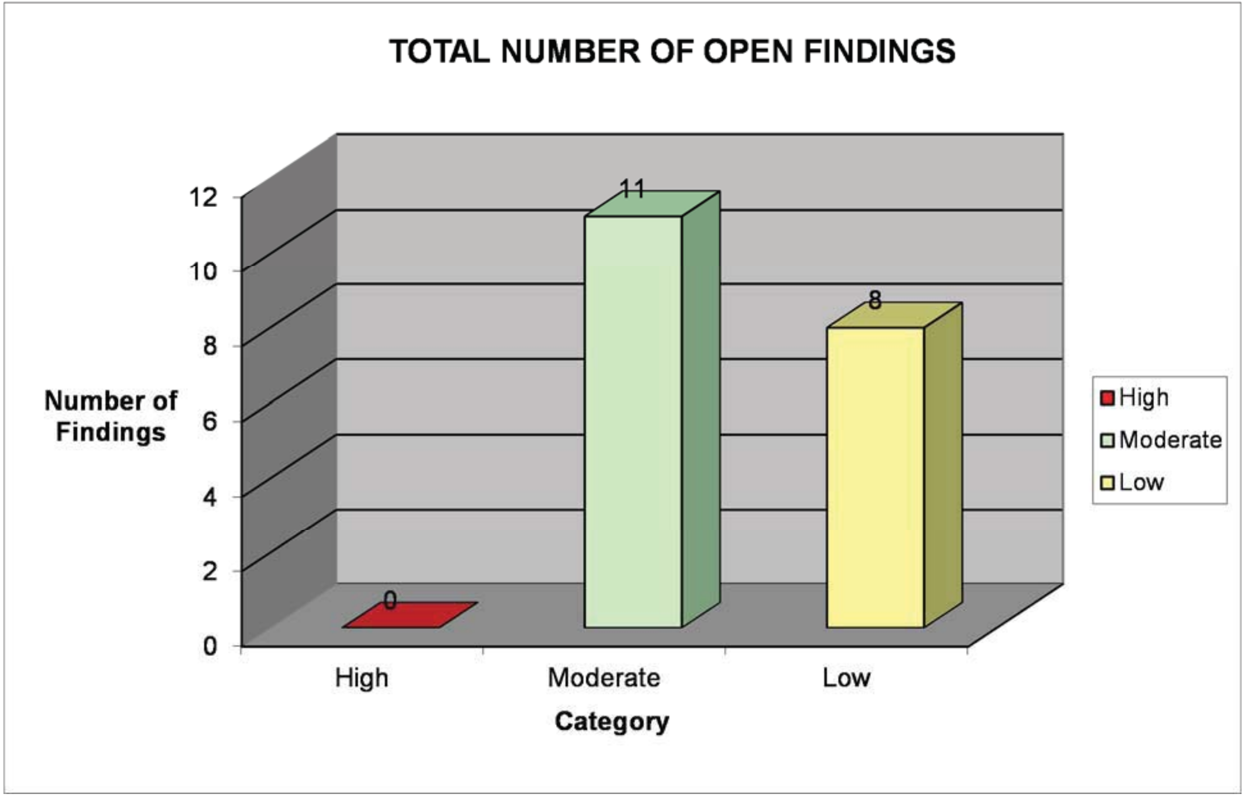

Figure 2. Open Findings by Risk Level

The HIX application has a "Moderate" Federal Information Processing Standard (FIPS) impact level since HIX contains sensitive information about persons and sensitive documents from insurance companies. 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:

- **Release Management Process:** The release management process, though documented in the SSP does not appear to match what staff is following. No documentation was provided to detail changes made or the approval of the changes by the release manager. Code has been released in to production which is available to the public, which was not functionally complete.
- **Functional Completeness:** The application at the time of testing was not functionally complete. Unit and smoke testing appeared to be the main focus of the development efforts instead of the security of the application, providing intuitive system feedback and the total end user experience. Multi-Factor authentication was not able to be tested because it was not integrated with EIDM at this point in time.
- **Access Control**: Security access rights granted to users need to be tightened and periodically reviewed. Access (b)(5), (b)(6), (b)(7)c, (b)(7)e was still active for users who no longer required it. Further, web application access controls needs to be refined to ensure

session and cookies are not misused. For example: Session Cookies should be better defined to ensure they only apply to the HIX application path, and are encrypted; Session Time outs need to be enforced to CMS Standards; Private IP addresses should be removed from view; CMS Approved warning banners should be shown; and Logout functionality should be implemented.

- **Application Security**: The HIX application had insecure configuration settings and multiple access control deficiencies in the tested environments. (b)(5)

  (b)(5)

- **System and Information Integrity**: (b)(5) (b)(5) (b)(5) CMS and CGI Federal implemented a fix to check data before writing it t(b)(5), (b)(6), (b)(7)c, (b)(7)e atabase tables; however, a best security practice is to validate all user input when it is entered. (b)(5) (b)(5)

- **Documentation Updates**: Although the SSP, ISRA, and Contingency Plan conformed to CMS methodologies, suggestions on areas to update with additional information were provided. For example, risks identified in the ISRA should be focused on the present security risks in the system not risks to the project timelines or ability to obtain an Authority to Operate. "Closed" or no longer relevant risks should be removed as they are no longer a risk. The SSP should reflect the "AS-IS" system, not the projected system. Detailed analysis of the SSP and ISRA were provided by MITRE.

1.6 SUMMARY OF RECOMMENDATIONS

(b)(5)

2 INTRODUCTION

A key provision of the Affordable Care Act (ACA) is the implementation of Insurance Marketplaces (Marketplaces). The Center for Consumer Information and Insurance Oversight (CCIIO) is responsible for providing guidance and oversight for the Marketplaces. A Marketplace is organized to help consumers and small businesses buy health insurance in a way that permits easy comparison of available plan options based on price, benefits and services, and quality. The ACA provides each State with the following options:

- Set up a State-Based Marketplace (SBM)
- Designate a non-profit entity to operate a State-Based Marketplace
- Collaborate with another state or a consortium to operate a Marketplace
- Defer to the Federally Facilitated Marketplace

The Marketplaces will carry out a number of functions required by the ACA, including certifying Qualified Health Plans (QHPs), administering Advance Premium Tax Credits (APTCs) and Cost Sharing Reductions (CSRs), and providing an easy-to-use website so that individuals can determine eligibility and enroll in health coverage. The Marketplaces will therefore be required to interact with a variety of stakeholders, including consumers, navigators, agents, brokers, employers, Health Plan Issuers, State-based Medicaid and Children's Health Insurance Programs (CHIPs), Federal agencies for verification checks, third-party data sources, and State Insurance Departments.

The HIX is comprised of several applications, commonly referred to as modules or business areas. Descriptions of these modules are listed below:

2.1.1 Plan Management (PM)

The Plan Management (PM) business area consists of business processes for acquiring, certifying, monitoring, renewing, and managing the withdrawal of qualified health plans (QHPs) and the Issuers that offer these plans for a given Marketplace. These areas are currently supported by a composite solution consisting of:

- Data submission templates (MS Excel-based) allowing States and Issuers or their representatives to download, populate, validate, and upload into the PM system various complex data sets detailing application, plan, and rate and benefits information.
- User interfaces and services for State and Issuer users to submit, review, modify, and attest to the information uploaded or provided directly via the user interface to support the application and rate and benefits collection process for a given marketplace or set of marketplaces.
- User interfaces and services for CMS personnel to review, monitor, and certify/decertify applications and plans submitted for approval in a given marketplace.
- System interfaces to existing CMS systems (e.g., Health Insurance Oversight System [HIOS]) to support streamlined data and profile collection and authentication.

- A system interface to CMS' portable document format (PDF) generation solution, (b)(5), (b)(6), (b)(7)c, (b)(7)e o create notices that are distributed to Issuers.

The PM application design is supported by a scalable, 3-tiered environment running on the CMS (b)(5), (b)(6), (b)(7)c, (b)(7)e database. The user interface design is based on the CMS.gov web brand including Healthcare.gov, CMS.gov, and Medicare.gov. It is Section 508 compliant and uses a Progressive Enhancement approach.

The Resubmission functionality provides the ability for Issuers to resubmit a plan for any of the following reasons:

- To address an application deficiency noted by HHS or the State
- To submit a data correction during the plan preview period
- To submit additional information for certification of stand-alone dental plans.

By initiating resubmission, the Issuer is temporarily invalidating the previously submitted QHP so that information related to one of the aforementioned factors above can be modified and resubmitted. Only QHPs with a *Cross Validation Completed* status may be resubmitted. Initiating resubmission for any module will change that module status to *Pending Submission* and all other modules to *Validation Completed.*

There is a Plan Preview ability that provides Issuers with the capability to view rates and plan details based on a set of subscriber and plan variance data selected by the user. The Summary page provides the user with the ability to select a specific IssuerID to preview their plan(s). The user can view an Issuer's submitted plans and rating scenarios by clicking on the View Plans button that corresponds to an Issuer in the Issuer table. The Rating Scenarios page allows the user to select plans and various inputs necessary for the rating engine to provide a rate(s).

The CMS Certification/Suppression module page serves two functions to CMS users. First, it provides CMS users with a daily report of all QHPs submitted to FFM, along with chief executive officer (CEO) contact information associated with each plan. The daily report includes all QHPs in the Marketplace and plans submitted through the National Association of Insurance Commissioners (NAIC) System for Electronic Rate and Form Filing (SERFF) and loaded into the Marketplace with a *Cross Validation Completed* status. Second, it provides CMS users the ability to set or change the status of a plan. CMS also uses this page to make any suppression changes to the plan. CMS users must select search criteria, using either IssuerID or PlanID, and click Search to display the results. The CMS user can then suppress a plan or cancel a plan suppression while adding or altering a suppression reason code.

2.1.2 **Eligibility & Enrollment (E&E)**

The Eligibility and Enrollment (E&E) module comprises services that are necessary to verify an applicant's eligibility for health insurance, plan selection and enrollment through the Marketplace. Eligibility determination includes, but is not limited to: income verification, citizenship verification, lawful presence verification, incarceration status verification, and verification of eligibility for other public minimum essential coverage or employer-sponsored minimum essential coverage health plans.

As applicants go through the steps to apply for insurance in the Marketplace, the applicants are prompted as to whether they qualify for a QHP, APTCs, CSRs, or other insurance such as State-based Medicaid or CHIP. Upon completion, health insurance benefits available to the applicant (and household members, if applicable) are displayed. Then the applicant can decide upon the insurance coverage that suits the household's needs, based on the information populated and verified in the Application.

FTI is collected in E&E and is stored in a (b)(5), (b)(6), (b)(7)c, (b)(7)e instance that is logically separated (b)(5), (b)(6), (b)(7)c, (b)(7)e The FFM three-tiered architecture includes a Presentation Zone, an Application Zone, and a Data Zone. The user interface (UI) is located in the Presentation Zone, while FTI is located in the Data Zone, with the Application Zone in between. The User Interface (UI) does not directly access FTI. The UI goes through the Application Zone to request FTI.

E&E has several distinct functions that are described below.

2.1.2.1 My Account

My Account is available to consumers (Public applicants or their designees). Specifically, consumers will be able to create a National Institute of Standards and Technology (NIST) Level of Assurance 2 (LOA2) account in the Marketplace, log in to the Marketplace using that LOA2 account, and perform maintenance activities on their account (e.g., update email address and reset password). The My Account page allows a Marketplace user to monitor and change all information related to the user's eligibility for an affordable insurance program. After a user registers and logs in, the user can update settings, grant other users access to their health insurance application (Application), review selection history, and report changes in circumstance.

2.1.2.2 Individual Application

The Individual Application captures the necessary information for the Marketplace to verify an applicant's eligibility for enrollment in a QHP. The applicant answers questions for citizenship status or lawful presence, residency information, and incarceration status to determine the applicant's eligibility to enroll in an affordable insurance plan. If a user requests financial assistance, the applicant answers additional questions to see if the applicant might be eligible for APTCs, CHIP, Medicaid, or CSR. Applicant-entered information triggers what web pages the applicant must complete to determine eligibility.

2.1.2.3 Plan Compare

When a user is ready to look at insurance plans the user accesses the Plan Compare pages. Plan Compare allows the user to view eligible plans and compare and view plan details. The user can customize and filter the plans displayed by selecting relevant criteria. For example, the user can filter by plan type, premium amount, maximum out-of-pocket expenses, deductible, CSR-eligible plans, metal level, and insurance company. Users can sort the results by premium and maximum out-of-pocket expenses. When users are ready to select a plan, they can add it to their cart from any page.

2.1.2.4 Eligibility Support Desktop

The Eligibility Support Desktop (ESD) provides the Eligibility Support Staff (ESS) members the ability to review the evidence documents provided by the consumer to resolve an inconsistency. The ESS worker can adjudicate the resolution of inconsistencies based on the authorized evidence documents delivered. As each evidence document is loaded into the ESD, a task is generated on the appropriate ESS member's Home page.

The task queue on the home page provides a list of all tasks that have been assigned to the ESS member based on the credentials entered; each ESS member is assigned a specific type of inconsistency or work type to review. Once the ESS member selects a task from the task queue, the ESD directs the worker to the Overall Records View page for the ESS member to start the review process on the Application with the inconsistency.

The Overall Record View page provides a high-level overview to the ESS worker of the Application's inconsistency and the relationship to the Applicant in terms of coverage, eligibility determinations, and pending inconsistencies. During the review and adjudication process, the ESS member can change the status of a document to sufficient or insufficient. The Applicant's Application status is updated to *Pending Additional Documentation*. During the review process, the ESS worker can reference the attested information during the individual or paper Application process.

2.1.2.5 Call Center Integration

The Next Generation Desktop (NGD) accesses FFM to retrieve basic history and information about the user's account, eligibility and enrollment history. FFM will expose the Call Center Representative (CCR) services directly to the Call Center application via th (b)(5), (b)(6), (b)(7)c, (b)(7)e the Application Zone and bypasses the Hub. For certain services, the CCRs use the same UI that the individuals use to assist a caller complete the Application eligibility and enrollment processes. Any update transactions go through the FFM UI.

2.1.2.6 Direct Enrollment

Consumers shopping for health insurance for themselves and/or their household members have the choice of enrolling in a QHP by accessing the FFM website directly, or by shopping via a partner website. The Direct Enrollment application programming interface (API) services facilitate integration between partner websites and FFM to support consumers shopping/enrolling in QHPs through partner websites.

FFM supports two models for partner websites to integrate their consumer shopping experience with FFM:

- Direct Enrollment API: Under this model, partner websites use FFM' User Interface services and Web services to implement a consumer's eligibility determination and plan shopping functions.
- Lead Generation API: Under this model, partner websites provide educational content and pre-sell their plans before transferring the consumer to the FFM website. The consumer completes all functions including eligibility determination, plan shopping and enrollment on FFM. However, the partner website specifies Issuer/Plan filters that FFM applies as part of the consumer's plan shopping. This model is offered as an alternative to

the Direct Enrollment API to support Issuers that may not be ready to implement the full Direct Enrollment API.

Federal Functions (Double Dipping)

Double Dipping includes verifying that an individual does not receive APTC/CSR from both a SBM and FFM. This process includes a check with the Enrollment Data Store (EDS) to determine if an individual is enrolled in a SBM and, if so, if they are already receiving ATPC/CSR through a SBM. If the individual is already receiving APTC/CSR, this process denies an individual APTC/CSR eligibility within FFM and prevents an individual from applying APTC/CSR in Plan Compare.

Federal Functions (EDS to store FFM and SBM Transactions)

FFM and SBM enrollment data sent to FFM will be stored in the Federal Exchange Program Systems (FEPS) EDS for the purpose of enabling Federal payments of APTC or CSR, and preventing duplicate APTCs across multiple Marketplaces. FFM will send a transaction to the issuer and a copy to the EDS directly. In the case of SBM, the Hub will facilitate the exchange of 834 transactions between parties. Specifically, the Hub will serve as the gateway for enrollment transactions between the SBM and EDS, accepting copies of enrollment transactions sent by SBMs to QHP issuers that offer coverage through SBMs.

2.1.2.7 Enrollment

Consumers can compare Plans, select a Plan, and enroll under a QHP. The enrollment information is sent to the Issuer for servicing. An enrollment is effectuated only after the consumer pays the first monthly premium to the Issuer. The consumer has the option to pay the first monthly premium as part of the enrollment process by being redirected to the Issuer's payment portal. All new enrollments will be sent to Issuers using X12 834 EDI transactions. Issuers will respond to FFM, also using the X12 834, with information on effectuation of the enrollment. If the first monthly premium is not received on time, the effectuation date may be moved back to the next applicable month.

2.1.2.8 Notices

The Notices for the Marketplace provide paper and electronic communication to the individual consumer. All Notices generated by the Marketplace are addressed and sent to the person designated to receive official communications, and are sent according to the communication preferences set by this person within My Account. A Notice is always sent in electronic format to the consumer's Bulletin Board and would also be printed and mailed if US Mail had been selected as a communications preference. When a Notice is sent electronically, an email or text message notification is sent to the contact person as well, informing them that there is official communication from the Marketplace waiting for them to review.

The following notices are scheduled for Day One:

- Eligibility Determination Notice
- ESD Custom Notice Template
- Data Sources Down Notice

- RIDP Failure Notice
- Request for More Info – Income
- Request for More Info – Step 3, 4 Immigration Status Notice

2.1.2.9 Mailing Contractor Integration

The Marketplace Mail Contractor Integration is responsible for transferring Notices flagged during the day for delivery by US Mail over to the mail contractor on a daily basis for printing. A batch process will retrieve the files to be sent and place them within a zip for transfer; there can be one or more zip files sent daily as there will be a maximum number of notice files that can be zipped into one. The Mail Contractor is responsible for printing and mailing the Notices and returning a response file to the Marketplace; this response file includes the confirmation of receipt and print date of each Notice file. The Marketplace stores the results received from the mail contractor.

2.1.3 **Financial Management (FM)**

Two Financial Management (FM) components are being implemented. They are:

- State Based Marketplace (SBM) Data Collection and Validation
- Preliminary and Final CSR Calculation

To support oversight and federal functions, SBMs are required to submit a subset of rate and benefit data for certified QHPs to FEPS via Enterprise File Transfer (EFT). For SBMs that use SERFF, data is extracted from SERFF. SBMs that do not use SERFF are required to extract the required data in the prescribed format described SBM Interface Control Document (ICD). All file submissions are full replacement files; all data elements should be sent with each submission.

Files are subjected to an initial file validation as well as data validations similar to those performed during the data collection in the FFM Plan Management templates. As part of the data intake process, the system obtains the EHB Portion of Allowed Claims, PM amount from the Unified Rate Review database based on the submitted Plan ID. Records that pass data validation are stored for future processes. Records that fail data validation are rejected. At the conclusion of the data validation process, an error report detailing failed data validations is sent to the SERFF/SBMs via EFT so data can be corrected and resubmitted as required. CMS has the ability to approve or disapprove the accepted records.

The submitted certified plan information is used to support future federal functions, including the calculation of advance CSR amounts and Edge Server processes.

The Advance CSR Payment Estimate process allows CMS to calculate and evaluate advance CSR payment amounts based on information submitted by Healthcare Marketplaces. At designated intervals, authorized CMS/CCIIO users will initiate the process to calculate advance CSR payment amounts within the FEPS.

Once the Advance CSR Payment Estimate process completes, CSV files containing the data required for outlier analysis are generated for rate analysis. Authorized users will review the results and have the ability to manually correct the calculations. The final amounts will undergo a review and approval process. Approved calculations will be submitted to Issuers and States via (b)(5), (b)(6), (b)(7)c, (b)(7)e via EFT.

2.2 Assessment Methodology

The MITRE Corporation (MITRE) was tasked with providing an application-only SCA of the HIX updates HIX modules that were not tested previously (e.g.PM, FM, and E&E modules). The physical location of the servers hosting the applications and databases is at th (b)(5), (b)(6), (b)(7)c, (b)(7)e (b)(5), (b)(6), (b)(7)c, (b)(7)e The assessment took place at the CGI Federal building located in Herndon, Va. The application was assessed August 19-30, 2013 and additionally September 16-19, 2013. Two separate test plans were drafted and submitted, one for each assessment. For the assessment in August 2013, please reference "*HIX August 2013 SCA FINAL_Test_Plan-08 21 2013.doc*". The September test is referenced as "*HIX-A September 2013 SCA Final_Test_Plan-09 17 2013.doc*". MITRE only considered the "as-is" application and did not consider future enhancements

2.2.1 **Joint Assessments**

The August and September assessments were joint assessments with other companies, systems and the IRS.

2.2.1.1 August 2013

The August 2013 assessment of HIX was run in parallel with the Data Services Hub (DSH) assessment. Joint meetings and daily out briefs were performed. Shared information and ad-hoc meetings with HIX and DSH groups were necessary to understand the integrations between the two systems.

The IRS and Booz Allen Hamilton (BAH) were onsite during the DSH and FFM assessments to evaluate FTI management and handling in the DSH and HIX systems. Funding of BAH and the IRS efforts were not provided under by MITRE's SCA contract. An instance of the HIX (b)(5), (b)(6), (b)(7)c, (b)(7)e assessed because of changes made since June 2013 to accommodate FTI. DSH and HIX provided documentation, SCA scans, questionnaires, demos, and findings were provided to the IRS and BAH at the request of CMS/CCIIO. IRS and BAH findings, reports and artifacts were not shared with MITRE and will not be reflected in this report. More information about IRS and BAH interactions can be found in the August 2013 test plan and daily out brief agendas.

2.2.1.2 September 2013

The September 2013 assessment of HIX was a joint assessment between MITRE and Blue Canopy/Deloitte for staff augmentation and contract transition efforts. Funding of Blue Canopy and Deloitte personnel was not provided by MITRE's SCA contract. Blue Canopy is the new SCA contractor as the Q2 2013 awarding of the SCA contract. Both groups collaborated with equal access to the HIX documentation, scans, interviews and past HIX assessments as directed by CMS/CCIIO. The application testing was divided between MITRE and Blue Canopy with separate reports being provided by both.

The purpose of this assessment was to do the following:

- Ensure that the system was in compliance with the *CMS Information Security (IS) Acceptable Risk Safeguards (ARS), Including CMS Minimum Security Requirements (CMSR), Version 1.0,*[1] *CMS Technical Reference Architecture, Version 2.0 (TRA),*[2] *CMS Minimum Security Configuration Standards for Operating Systems, Version 4.0,*[3] *CMS Policy for the Information Security Program,*[4] *and CMS Business Partner Systems Security Manual, Version 10.6.*[5]
- Ensure that the underlying infrastructure was securely implemented.
- Determine if the application was securely maintained.
- Ensure that the database was configured properly.

2.3 Assessment Summary

The August and September 2013 assessments of the HIX did not assess functionally complete versions of the Eligibility & Enrollment (E&E), Financial Management (FM), and Plan Management (PM) modules in the same environments. Documentation provided divulged some known functional limitations and omissions due to the software still being developed. The provided list omitted numerous issues that required investigation to resolve. Workarounds to the components being tested were provided that impacted end to end MITRE test cases.

MITRE was unable to confidently test the Confidentiality and Integrity of the HIX system in full. The majority of the MITRE's testing efforts were focused 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.

- **Testing environments and module interconnections were not ready for the SCA**. Specifically during the September assessment, MITRE was given three different environments to test in (b)(5), (b)(6), (b)(7)c, (b)(7)e at various times to compensate for interconnections not be made. These environments were not vetted or tested prior to the onsite to make sure the HIX workflows were functional. Inputted information in most instances was unable to be validated as needed by the work flow to proceed to the next step in the HIX Workflows.

- **Valid Test data was not provided prior for testing**. MITRE requested that test data be prepopulated in the HIX application's database prior to the onsite so testers could

[1] https://www.cms.gov/informationsecurity/downloads/ARS_App_A_CMSR_HIGH.pdf (08/31/2010), https://www.cms.gov/informationsecurity/downloads/ARS_App_B_CMSR_Moderate.pdf(08/31/2010), https://www.cms.gov/informationsecurity/downloads/ARS_App_C_CMSR_Low.pdf(08/31/2010).

[2] TRA and Supplements can be found on CMS's internal website (November 24, 2009).

[3] http://www.cms.hhs.gov/cbt/downloads/is_baseline_configs.pdf (February 4, 2010). Only available to authorized users of CMS systems.

[4] http://www.cms.hhs.gov/informationsecurity/downloads/PISP.pdf, Version CMS-CIO-POL-SEC02-03.

[5] http://www.cms.gov/manuals/downloads/117_systems_security.pdf (July 17, 2009).

start testing anywhere in the workflow of the application. This was never provided. In a three step process (1. Account Creation, 2. Individual Application creation and 3. Plan Compare) MITRE had to create an Account and Application every time to run one test case for Plan Compare testing. Each test case took about 45 minutes to an hour to set up. Specifically, for an Application for a family of four, there is about 400 data elements (name, address, SSN, etc.) that need to be entered in the Individual Application. There are also system validations and calls to other applications (SSN validation) that need to be performed.

- **Environment availability was not consistent**. Several times during the SCA the testing environments "went down" due to DSH, EIDM or HIOS systems needed to be taken off line or rebooted. These events would occur without warning and only after the systems were taken off line was MITRE informed. This caused many outages and black out windows for SCA testing because the system was functionally unusable.

- **Environments were not dedicated to SCA testing.** It was reported that other groups such as issues were working in the provided testing environment. CMS instructed MITRE that SCA efforts to interrupt the availability of the system, (b)(5), (b)(6), (b)(7)c, (b)(7)e attacks, were not to be performed.

3 DETAILED FINDINGS

Section 3 provides a descriptive analysis of the vulnerabilities identified through the comprehensive SCA process. Each vulnerability is thoroughly explained, specific risks to the continued operations of CMS information systems are identified, and the impact of each risk is analyzed as a business case. The Business Risks also contain suggested corrective actions for closing or reducing the impact of each vulnerability.

Preceding the detailed Business Risks, the methodologies for performing the comprehensive SCA and reporting test results are presented. These sections explain the comprehensive SCA process and describe how the Business Risk Level, Ease-of-Fix, and Estimated Work Effort metrics have been assessed.

3.1 Methodology for Application-Only Security Control Assessment

The overall comprehensive methodology for this assessment consisted of a multi-prong approach in which MITRE conducted a technical vulnerability assessment, a system configuration audit, policy compliance audit, and a documentation review. This approach provided MITRE with an accurate understanding of the HIX PM, FM, and E&E modules to determine if it was configured according to CMS standards. The main objectives of the application-only SCA were to identify the following:

- Vulnerabilities and their potential impact
- Weak system configuration settings that if not changed could compromise the CIA of system data

- Where established CMS security policies have not been followed
- Major discrepancies found in the documentation of the installed systems
- Any weaknesses in the Configuration Management (CM) process
- Any weakness found in HIX PM, FM, and E&E modules Program Management

3.1.1 **Application-Only Vulnerability Assessment**

The application-only vulnerability assessment evaluated the system's vulnerability to insider, intranet, and network-based attacks, as well as weaknesses in the management and operational areas of the Office of Consumer Information and Insurance Oversight (OCIIO), and CGI-Federal Security Programs. To accomplish this objective, MITRE developed an understanding of how the system was configured to determine what an adversary could learn about, and subsequently exploit, in the operational environment.

The application-only SCA was conducted with full knowledge of the system, products, configurations, and topology. To determine the system configuration and complete a vulnerability assessment of the HIX PM, FM, and E&E modules, MITRE's SCA looked for the following:

- Improper, weak, or vulnerable configurations
- Non-standard configurations
- Published or known weaknesses, bugs, advisories, and security alerts about specific hardware, software, and networking products used in the system
- Common or known attacks against the specific hardware, software, and networking products used in the system
- Failure to comply with CMS security policies and procedures

3.1.2 **Tests and Analyses**

The application-only SCA included a number of tests that methodically analyzed the HIX PM, FM, and E&E modules. The types of tests and analyses MITRE fully or in-part performed during this assessment included the following:

- **Application Assessment—**subjected the applications to manual and automated testing to ensure the CIA of data processed by the application
- **Database Scanning—**subjected the underlying database to automated scripts to discover any vulnerabilities in the database configuration
- **System Configuration Assessment**—ran automated scripts and used direct observation to analyze the configuration of network components
- **Best Engineering Judgment and Various Ad Hoc Tests**—verified that specific requirements, previous recommendations, and conditions had been satisfied
- **Personnel Interviews**—interviewed various personnel involved with the daily operational maintenance of the HIX PM, FM, and E&E modules, as well as other personnel tasked with protecting the system

3.1.3 **Tools**

MITRE will work with CMS CGI Federal staff to ensure that industry standard best practices are reflected in CMS's system architecture design. The work performed on this task was accomplished on MITRE-furnished auditing equipment. The tools used by MITRE during the assessment are listed below:

- **Burp Suite** (http://portswigger.net/burp/)—integrated platform for performing security testing of Web applications.
- **MITRE host-based and database scripts**—scripts developed with the contribution and experience of MITRE's vulnerability and penetration testers. Versions have been developed for both Windows and Unix-based operating systems. With the assistance of SysAdmins, the MITRE Assessment Team uses these scripts to audit operating system security configurations and identify misconfigurations
- **Mozilla and Firefox Web Browsers** (http://www.mozilla.org)—open-source Web-based browsers used to manually browse and inspect the Web application and associated forms
- (b)(5), (b)(6), (b)(7)c, (b)(7)e —premier open-source vulnerability assessment tool
- **Paros** (http://www.parosproxy.org (b)(5), (b)(6), (b)(7)c, (b)(7)e sed to evaluate Web application security (similar to Achilles)
- **Wireshark** (http://www.wireshark.org)—open-source, GUI network protocol analyzer

3.2 Methodology for Security Test Reporting

The format and content of this report has been developed in accordance with the *CMS Reporting Procedure for Information Security (IS) Assessments, Version 5.0*.[6] The CMS Reporting Standard requires that a Risk Level assessment value be assigned to each Business Risk in order to provide a guideline by which to understand the procedural or technical significance of each finding. Further, an Ease-of-Fix and Estimated Work Effort value must be assigned to each Business Risk to demonstrate how simple or difficult it might be to complete the reasonable and appropriate corrective actions required to close or reduce the impact of each vulnerability. Based on an understanding of the vulnerabilities identified, current CMS implementation of the underlying technology, and the assessment guidelines contained with the *CMS Reporting Procedure for Information Security (IS) Assessments* document, MITRE has assigned these values to each Business Risk.

3.2.1 Risk Level Assessment

Each Business Risk has been assigned a Risk Level value of High, Moderate, or Low. The rating is, in actuality, an assessment of the priority with which each Business Risk will be viewed. The definitions in Table 1 apply to risk level assessment values.

Table 1. Risk Level Definitions

Rating	Definition of Risk Rating

[6] http://www.cms.gov/informationsecurity/downloads/Assessment_Rpting_Procedure.pdf (March 19, 2009).

Rating	Definition of Risk Rating
High	Exploitation of the technical or procedural vulnerability will cause substantial harm to CMS business processes. Significant political, financial, and legal damage is likely to result
Moderate	Exploitation of the technical or procedural vulnerability will significantly impact the confidentiality, integrity and/or availability of the system or data. Exploitation of the vulnerability may cause moderate financial loss or public embarrassment to CMS
Low	Exploitation of the technical or procedural vulnerability will cause minimal impact to CMS operations. The confidentiality, integrity and availability of sensitive information are not at risk of compromise. Exploitation of the vulnerability may cause slight financial loss or public embarrassment
Informational	An “Informational” finding, is a risk that has been identified during this assessment which is reassigned to another major application (MA) or General Support System (GSS). The finding must already exist and be open for the reassigned MA or GSS. The informational finding will be noted in a separate section in the final SCA report, but will not be the responsibility of the assessed application to create a Corrective Action Plan, as it is reassigned to the MA or GSS.

3.2.2 Ease-of-Fix Assessment

Each Business Risk has been assigned an Ease-of-Fix value of Easy, Moderately Difficult, Very Difficult, or No Known Fix. The Ease-of-Fix value is an assessment of how difficult or easy it will be to complete reasonable and appropriate corrective actions required to close or reduce the impact of the vulnerability. The definitions in Table 2 apply to the Ease-of-Fix values.

Table 2. Ease-of-Fix Definitions

Rating	Definition of Ease-of-Fix Rating
Easy	The corrective action(s) can be completed quickly with minimal resources and without causing disruption to the system, or data
Moderately Difficult	Remediation efforts will likely cause a noticeable service disruption: • A vendor patch or major configuration change may be required to close the vulnerability • An upgrade to a different version of the software may be required to address the impact severity • The system may require a reconfiguration to mitigate the threat exposure • Corrective action may require construction or significant alterations to the manner in which business is undertaken
Very Difficult	The high risk of substantial service disruption makes it impractical to complete the corrective action for mission critical systems without careful scheduling: • An obscure, hard-to-find vendor patch may be required to close the vulnerability • Significant, time-consuming configuration changes may be required to address the threat exposure or impact severity • Corrective action requires major construction or redesign of an entire business process

Rating	Definition of Ease-of-Fix Rating
No Known Fix	No known solution to the problem currently exists. The risk may require the business owner to: • Discontinue use of the software or protocol • Isolate the information system within the enterprise, thereby eliminating reliance on the system In some cases, the vulnerability is due to a design-level flaw that cannot be resolved through the application of vendor patches or the reconfiguration of the system. If the system is critical and must be used to support on-going business functions, no less than quarterly monitoring shall be conducted by the business owner and reviewed by CMS IS Management to validate that security incidents have not occurred

3.2.3 Estimated Work Effort Assessment

Each Business Risk has been assigned an Estimated Work Effort value of Minimal, Moderate, Substantial, or Unknown. The Estimated Work Effort value is an assessment of the extent of resources required to complete reasonable and appropriate corrective actions. The definitions in Table 3 apply to the Estimated Work Effort values.

Table 3. Estimated Work Effort Definitions

Rating	Definition of Estimated Work Effort Rating
Minimal	A limited investment of time (i.e., roughly three days or less) is required of a single individual to complete the corrective action(s)
Moderate	A moderate time commitment, up to several weeks, is required of multiple personnel to complete all corrective actions
Substantial	A significant time commitment, up to several months, is required of multiple personnel to complete all corrective actions. Substantial work efforts include the redesign and implementation of CMS network architecture and the implementation of new software, with associated documentation, testing, and training, across multiple CMS organizational units
Unknown	The time necessary to reduce or eliminate the vulnerability is currently unknown

3.2.4 CMS FISMA Controls Tracking System Names

To ensure that the final security controls/findings worksheet can be properly loaded into the CMS FISMA Controls Tracking System (CFACTS), the following system name has been used to populate the System Name field in the Final Management Worksheet delivered as an attachment to this report.

Table 4. CFACTS System Names

CFACTS System Names
"HIX" Pre-Sept 2013 *"FFM" Post Sept 2013*

3.3 Business Risks

Management, operational, and technical vulnerabilities representing risks to the secure operation of the HIX are detailed as findings in this section. Business Risks within this section are technical or procedural in nature, and may result directly in unauthorized access.

To support the *CMS Reporting Procedure for Information Security (IS) Assessments,* the vulnerabilities are ordered in a format that will enable CMS to develop an efficient and workable action plan to remediate all risks. The Business Risks are ordered first by Risk Level from High Risk to Low Risk and then by Estimated Work Effort from Substantial to Minimal. This format will help CMS identify critical risks that must be immediately addressed with little time and effort. Each discussion section identifies the servers or whether the Production or Test environment is impacted by the vulnerability. CMS should initially focus on addressing critical risks that impact the Production environment.

3.3.1. BUSINESS RISK	(b)(5)

Applicable Standards:

NIST Security Control Families: Access Control (AC)

Reference: AC-6

Risk Level: (Risk Level is High, Moderate, or Low)

HIGH

Ease-of-Fix: (Ease-of-Fix is Easy, Moderately Difficult, Very Difficult, or No Known Fix)

Moderately Difficult

Estimated Work Effort: (Estimated Work Effort is Minimal, Moderate, Substantial, or Unknown; or a time estimate based on level of commitment and an adequate skill set)

Moderate

Description:

3.3.1 FFM 10112013

Finding

(b)(5)

This risk is mapped to row 24 from the initial collection spreadsheet.

(b)(5)

(b)(5)

Recommended Corrective Action(s):

(b)(5)

3.3.2. BUSINESS RISK

(b)(5)

Applicable Standards:

NIST Security Control Families: System and Communications Protection (SC)

Reference: SC-10

Risk Level: (Risk Level is High, Moderate, or Low)

High

Ease-of-Fix: (Ease-of-Fix is Easy, Moderately Difficult, Very Difficult, or No Known Fix)

Easy

Estimated Work Effort: (Estimated Work Effort is Minimal, Moderate, Substantial, or Unknown; or a time estimate based on level of commitment and an adequate skill set)

Minimal

Description:

3.3.2 FFM 10112013

Finding

(b)(5)

This risk is mapped to row 1 from the initial collection spreadsheet.

(b)(5)

(b)(5)

(b)(5)

(b)(5)

Recommended Corrective Action(s):

(b)(5)

3.3.3. BUSINESS RISK

(b)(5)

Applicable Standards:

NIST Security Control Families: Access Control (AC)

Reference: AC-11

Risk Level: (Risk Level is High, Moderate, or Low)

Moderate

Ease-of-Fix: (Ease-of-Fix is Easy, Moderately Difficult, Very Difficult, or No Known Fix)

Moderately Difficult

Estimated Work Effort: (Estimated Work Effort is Minimal, Moderate, Substantial, or Unknown; or a time estimate based on level of commitment and an adequate skill set)

Moderate

Description:

3.3.3 FFM 10112013

Finding

(b)(5)

This risk is mapped to row 6 from the initial collection spreadsheet.

(b)(5)

(b)(5)

Recommended Corrective Action(s):

(b)(5)

3.3.4. BUSINESS RISK	(b)(5)

Applicable Standards:

NIST Security Control Families: Systems and Communications Protection (SC)

Reference: SC-4

Risk Level: (Risk Level is High, Moderate, or Low)

Moderate

Ease-of-Fix: (Ease-of-Fix is Easy, Moderately Difficult, Very Difficult, or No Known Fix)

Moderately Difficult

Estimated Work Effort: (Estimated Work Effort is Minimal, Moderate, Substantial, or Unknown; or a time estimate based on level of commitment and an adequate skill set)

Moderate

Description:

3.3.4 FFM 10112013

Finding

(b)(5)

This risk is mapped to row 9 from the initial collection spreadsheet.

(b)(5)

(b)(5)

(b)(5)

(b)(5)

Recommended Corrective Action(s):

(b)(5)

3.3.5. BUSINESS RISK

(b)(5)

Applicable Standards:

NIST Security Control Families: System and Communications Protection (SC)

Reference: SC-13(1)

Risk Level: (Risk Level is High, Moderate, or Low)

Moderate

Ease-of-Fix: (Ease-of-Fix is Easy, Moderately Difficult, Very Difficult, or No Known Fix)

Moderately Difficult

Estimated Work Effort: (Estimated Work Effort is Minimal, Moderate, Substantial, or Unknown; or a time estimate based on level of commitment and an adequate skill set)

Moderate

Description:

3.3.5 FFM 10112013

Finding

(b)(5)

This risk is mapped to row 10 from the initial collection spreadsheet.

(b)(5)

(b)(5)

Recommended Corrective Action(s):

(b)(5)

3.3.6. BUSINESS RISK	(b)(5) [redacted]

Applicable Standards:

NIST Security Control Families: System and Information Integrity (SI)

Reference: SI-10

Risk Level: (Risk Level is High, Moderate, or Low)

Moderate

Ease-of-Fix: (Ease-of-Fix is Easy, Moderately Difficult, Very Difficult, or No Known Fix)

Moderately Difficult

Estimated Work Effort: (Estimated Work Effort is Minimal, Moderate, Substantial, or Unknown; or a time estimate based on level of commitment and an adequate skill set)

Moderate

Description:

3.3.6 FFM 10112013

Finding

(b)(5) [redacted]

This risk is mapped to row 11 from the initial collection spreadsheet.

(b)(5) [redacted]

(b)(5)

Recommended Corrective Action(s):

(b)(5)

3.3.7. BUSINESS RISK	(b)(5)

Applicable Standards:

NIST Security Control Families: Access Control (AC)

Reference: AC-6

Risk Level: (Risk Level is High, Moderate, or Low)

Moderate

Ease-of-Fix: (Ease-of-Fix is Easy, Moderately Difficult, Very Difficult, or No Known Fix)

Moderately Difficult

Estimated Work Effort: (Estimated Work Effort is Minimal, Moderate, Substantial, or Unknown; or a time estimate based on level of commitment and an adequate skill set)

Moderate

Description:

3.3.7 FFM 10112013

Finding

(b)(5)

This risk is mapped to row 19 from the initial collection spreadsheet.

(b)(5)

(b)(5)

Recommended Corrective Action(s):

(b)(5)

3.3.8. BUSINESS RISK	(b)(5)

Applicable Standards:

NIST Security Control Families: System and Information Integrity (SI)

Reference: SI-3, SI-10

Risk Level: (Risk Level is High, Moderate, or Low)

Moderate

Ease-of-Fix: (Ease-of-Fix is Easy, Moderately Difficult, Very Difficult, or No Known Fix)

Easy

Estimated Work Effort: (Estimated Work Effort is Minimal, Moderate, Substantial, or Unknown; or a time estimate based on level of commitment and an adequate skill set)

Moderate

Description:

3.3.8 FFM 10112013

Finding

(b)(5)

This risk is mapped to row 25 from the initial collection spreadsheet.

(b)(5)

Recommended Corrective Action(s):

(b)(5)

3.3.9. BUSINESS RISK (b)(5)

Applicable Standards:

NIST Security Control Families: System and Communication Protection (SC)

Reference: SC-9

Risk Level: (Risk Level is High, Moderate, or Low)

Moderate

Ease-of-Fix: (Ease-of-Fix is Easy, Moderately Difficult, Very Difficult, or No Known Fix)

Easy

Estimated Work Effort: (Estimated Work Effort is Minimal, Moderate, Substantial, or Unknown; or a time estimate based on level of commitment and an adequate skill set)

Minimal

Description:

3.3.9 FFM 10112013

Finding

(b)(5)

This risk is mapped to row 12 from the initial collection spreadsheet.

(b)(5)

(b)(5)

Recommended Corrective Action(s):

(b)(5)

3.3.10. BUSINESS RISK	(b)(5)

Applicable Standards:

NIST Security Control Families: System and Communication Protection (SC)

Reference: SC-9

Risk Level: (Risk Level is High, Moderate, or Low)

Moderate

Ease-of-Fix: (Ease-of-Fix is Easy, Moderately Difficult, Very Difficult, or No Known Fix)

Easy

Estimated Work Effort: (Estimated Work Effort is Minimal, Moderate, Substantial, or Unknown; or a time estimate based on level of commitment and an adequate skill set)

Minimal

Description:

3.3.10 FFM 10112013

Finding

(b)(5)

This risk is mapped to row 13 from the initial collection spreadsheet.

(b)(5)

(b)(5)

Recommended Corrective Action(s):

(b)(5)

3.3.11. BUSINESS RISK	(b)(5)

Applicable Standards:

NIST Security Control Families: Access Control (AC)

Reference: AC-3

Risk Level: (Risk Level is High, Moderate, or Low)

Moderate

Ease-of-Fix: (Ease-of-Fix is Easy, Moderately Difficult, Very Difficult, or No Known Fix)

Easy

Estimated Work Effort: (Estimated Work Effort is Minimal, Moderate, Substantial, or Unknown; or a time estimate based on level of commitment and an adequate skill set)

Minimal

Description:

3.3.11 FFM 10112013

Finding

(b)(5)

This risk is mapped to row 20 from the initial collection spreadsheet.

(b)(5)

(b)(5)

Recommended Corrective Action(s):

(b)(5)

3.3.12. BUSINESS RISK	(b)(5)

Applicable Standards:

NIST Security Control Families: Access Control (AC)

Reference: AC-2

Risk Level: (Risk Level is High, Moderate, or Low)

Moderate

Ease-of-Fix: (Ease-of-Fix is Easy, Moderately Difficult, Very Difficult, or No Known Fix)

Easy

Estimated Work Effort: (Estimated Work Effort is Minimal, Moderate, Substantial, or Unknown; or a time estimate based on level of commitment and an adequate skill set)

Minimal

Description:

3.3.12 FFM 10112013

Finding

(b)(5)

This risk is mapped to row 23 from the initial collection spreadsheet.

(b)(5)

(b)(5)

(b)(5)

Recommended Corrective Action(s):

(b)(5)

3.3.13. BUSINESS RISK	(b)(5)

Applicable Standards:

NIST Security Control Families: System and Communication Protection (SC)

Reference: SC-23

Risk Level: (Risk Level is High, Moderate, or Low)

Moderate

Ease-of-Fix: (Ease-of-Fix is Easy, Moderately Difficult, Very Difficult, or No Known Fix)

Easy

Estimated Work Effort: (Estimated Work Effort is Minimal, Moderate, Substantial, or Unknown; or a time estimate based on level of commitment and an adequate skill set)

Minimal

Description:

3.3.13 FFM 10112013

Finding

(b)(5)

This risk is mapped to row 26 from the initial collection spreadsheet.

(b)(5)

(b)(5)

(b)(5)

Recommended Corrective Action(s):

(b)(5)

(b)(5)

3.3.14. BUSINESS RISK	(b)(5)

Applicable Standards:

NIST Security Control Families: System and Communication Protection (SC)

Reference: SC-7

Risk Level: (Risk Level is High, Moderate, or Low)

Moderate

Ease-of-Fix: (Ease-of-Fix is Easy, Moderately Difficult, Very Difficult, or No Known Fix)

Moderate

Estimated Work Effort: (Estimated Work Effort is Minimal, Moderate, Substantial, or Unknown; or a time estimate based on level of commitment and an adequate skill set)

Minimal

Description:

3.3.14 FFM 10112013

Finding

(b)(5)

This risk is mapped to row 27 from the initial collection spreadsheet.

(b)(5)

(b)(5)

(b)(5)

Recommended Corrective Action(s):

(b)(5)

(b)(5)

3.3.15. BUSINESS RISK	(b)(5)

Applicable Standards:

NIST Security Control Families: Configuration Management (CM)

Reference: CM-7

Risk Level: (Risk Level is High, Moderate, or Low)

Low

Ease-of-Fix: (Ease-of-Fix is Easy, Moderately Difficult, Very Difficult, or No Known Fix)

Moderately Difficult

Estimated Work Effort: (Estimated Work Effort is Minimal, Moderate, Substantial, or Unknown; or a time estimate based on level of commitment and an adequate skill set)

Moderate

Description:

3.3.15 FFM 10112013

Finding

(b)(5)

This risk is mapped to row 14 from the initial collection spreadsheet.

(b)(5)

(b)(5)

(b)(5) [redacted]

Recommended Corrective Action(s):

(b)(5) [redacted]

(b)(5) [redacted]

3.3.16. BUSINESS RISK	(b)(5)

Applicable Standards:

NIST Security Control Families: Access Control (AC)

Reference: AC-4

Risk Level: (Risk Level is High, Moderate, or Low)

Low

Ease-of-Fix: (Ease-of-Fix is Easy, Moderately Difficult, Very Difficult, or No Known Fix)

Moderately Difficult

Estimated Work Effort: (Estimated Work Effort is Minimal, Moderate, Substantial, or Unknown; or a time estimate based on level of commitment and an adequate skill set)

Moderate

Description:

3.3.16 FFM 10112013

Finding

(b)(5)

This risk is mapped to row 15 from the initial collection spreadsheet.

(b)(5)

(b)(5)

(b)(5)

Recommended Corrective Action(s):

(b)(5)

(b)(5)

3.3.17. BUSINESS RISK	(b)(5)

Applicable Standards:

NIST Security Control Families: System and Communications Protection (SC)

Reference: SC-23

Risk Level: (Risk Level is High, Moderate, or Low)

Low

Ease-of-Fix: (Ease-of-Fix is Easy, Moderately Difficult, Very Difficult, or No Known Fix)

Easy

Estimated Work Effort: (Estimated Work Effort is Minimal, Moderate, Substantial, or Unknown; or a time estimate based on level of commitment and an adequate skill set)

Minimal

Description:

3.3.17 FFM 10112013

Finding

(b)(5)

This risk is mapped to row 16 from the initial collection spreadsheet.

(b)(5)

(b)(5)

Recommended Corrective Action(s):

(b)(5)

3.3.18. BUSINESS RISK	(b)(5)

Applicable Standards:

NIST Security Control Families: Access Control (AC)

Reference: AC-8

Risk Level: (Risk Level is High, Moderate, or Low)

Low

Ease-of-Fix: (Ease-of-Fix is Easy, Moderately Difficult, Very Difficult, or No Known Fix)

Easy

Estimated Work Effort: (Estimated Work Effort is Minimal, Moderate, Substantial, or Unknown; or a time estimate based on level of commitment and an adequate skill set)

Minimal

Description:

3.3.18 FFM 10112013

Finding

(b)(5)

This risk is mapped to row 17 from the initial collection spreadsheet.

(b)(5)

(b)(5)

(b)(5)

Recommended Corrective Action(s):

(b)(5)

(b)(5)

3.3.19. BUSINESS RISK	(b)(5)

Applicable Standards:

NIST Security Control Families: System & Information Integrity (SI)

Reference: SI-11

Risk Level: (Risk Level is High, Moderate, or Low)

Low

Ease-of-Fix: (Ease-of-Fix is Easy, Moderately Difficult, Very Difficult, or No Known Fix)

Easy

Estimated Work Effort: (Estimated Work Effort is Minimal, Moderate, Substantial, or Unknown; or a time estimate based on level of commitment and an adequate skill set)

Minimal

Description:

3.3.19 FFM 10112013

Finding

(b)(5)

This risk is mapped to row 18 from the initial collection spreadsheet.

(b)(5)

(b)(5)

(b)(5)

Recommended Corrective Action(s):

(b)(5)

(b)(5)

3.3.20. BUSINESS RISK	(b)(5)

Applicable Standards:

NIST Security Control Families: Access Control (AC)

Reference: AC-6

Risk Level: (Risk Level is High, Moderate, or Low)

Low

Ease-of-Fix: (Ease-of-Fix is Easy, Moderately Difficult, Very Difficult, or No Known Fix)

Easy

Estimated Work Effort: (Estimated Work Effort is Minimal, Moderate, Substantial, or Unknown; or a time estimate based on level of commitment and an adequate skill set)

Minimal

Description:

3.3.20 FFM 10112013

Finding

(b)(5)

This risk is mapped to row 21 from the initial collection spreadsheet.

(b)(5)

(b)(5)

(b)(5)

(b)(5)

Recommended Corrective Action(s):

(b)(5)

(b)(5)

3.3.21. BUSINESS RISK	(b)(5)

Applicable Standards:

NIST Security Control Families: Access Control (AC)

Reference: AC-6

Risk Level: (Risk Level is High, Moderate, or Low)

Low

Ease-of-Fix: (Ease-of-Fix is Easy, Moderately Difficult, Very Difficult, or No Known Fix)

Easy

Estimated Work Effort: (Estimated Work Effort is Minimal, Moderate, Substantial, or Unknown; or a time estimate based on level of commitment and an adequate skill set)

Minimal

Description:

3.3.21 FFM 10112013

Finding

(b)(5)

This risk is mapped to row 22 from the initial collection spreadsheet.

(b)(5)

(b)(5)

(b)(5)

Recommended Corrective Action(s):

(b)(5)

(b)(5)

3.3.22. BUSINESS RISK

(b)(5)

Applicable Standards:

NIST Security Control Families: System and Communications Protection Policy and Procedu

Reference: SC-5

Risk Level: (Risk Level is High, Moderate, or Low)

Low

Ease-of-Fix: (Ease-of-Fix is Easy, Moderately Difficult, Very Difficult, or No Known Fix)

Easy

Estimated Work Effort: (Estimated Work Effort is Minimal, Moderate, Substantial, or Unknown; or a time estimate based on level of commitment and an adequate skill set)

Minimal

Description:

3.3.22 FFM 10112013

Finding

(b)(5)

This risk is mapped to row 28 from the initial collection spreadsheet.

(b)(5)

(b)(5)

Recommended Corrective Action(s):

(b)(5)

(b)(5)

3.4 Informational Risks

(b)(5)

3.4.1 **Business Risk**	(b)(5)

Applicable Standards:

NIST Security Control Families: Planning (PL)

Reference: PL-2

Risk Level: (Risk Level is High, Moderate, or Low)

Moderate

Ease-of-Fix: (Ease-of-Fix is Easy, Moderately Difficult, Very Difficult, or No Known Fix)

Easy

Estimated Work Effort: (Estimated Work Effort is Minimal, Moderate, Substantial, or Unknown; or a time estimate based on level of commitment and an adequate skill set)

Moderate

Description:

3.4.1 FFM 10112013

Finding

(b)(5)

This risk is mapped to row 2 from the initial collection spreadsheet.

(b)(5)

(b)(5)

Recommended Corrective Action(s):

(b)(5)

(b)(5)

3.4.2 **Business Risk**	(b)(5)

Applicable Standards:

NIST Security Control Families: Contingency Planning (CP)

Reference: CP-4

Risk Level: (Risk Level is High, Moderate, or Low)

Moderate

Ease-of-Fix: (Ease-of-Fix is Easy, Moderately Difficult, Very Difficult, or No Known Fix)

Easy

Estimated Work Effort: (Estimated Work Effort is Minimal, Moderate, Substantial, or Unknown; or a time estimate based on level of commitment and an adequate skill set)

Moderate

Description:

3.4.2 FFM 10112013

Finding

(b)(5)

This risk is mapped to row 5 from the initial collection spreadsheet.

(b)(5)

(b)(5)

Recommended Corrective Action(s):

(b)(5)

(b)(5)

3.4.3 **Business Risk**	(b)(5)

Applicable Standards:

NIST Security Control Families: Risk Assessment (RA)

Reference: RA-3

Risk Level: (Risk Level is High, Moderate, or Low)

Moderate

Ease-of-Fix: (Ease-of-Fix is Easy, Moderately Difficult, Very Difficult, or No Known Fix)

Easy

Estimated Work Effort: (Estimated Work Effort is Minimal, Moderate, Substantial, or Unknown; or a time estimate based on level of commitment and an adequate skill set)

Minimal

Description:

3.4.3 FFM 10112013

Finding

(b)(5)

This risk is mapped to row 3 from the initial collection spreadsheet.

(b)(5)

(b)(5)

(b)(5)

Recommended Corrective Action(s):

(b)(5)

3.4.4 Business Risk

(b)(5)

Applicable Standards:

NIST Security Control Families: Contingency Planning (CP)

Reference: CP-2

Risk Level: (Risk Level is High, Moderate, or Low)

Moderate

Ease-of-Fix: (Ease-of-Fix is Easy, Moderately Difficult, Very Difficult, or No Known Fix)

Easy

Estimated Work Effort: (Estimated Work Effort is Minimal, Moderate, Substantial, or Unknown; or a time estimate based on level of commitment and an adequate skill set)

Minimal

Description:

3.4.4 FFM 10112013

Finding

(b)(5)

This risk is mapped to row 4 from the initial collection spreadsheet.

(b)(5)

(b)(5)

Recommended Corrective Action(s):

(b)(5)

3.4.5 Business Risk

(b)(5)

Applicable Standards:

NIST Security Control Families: Access Control (AC)

Reference: AC-10

Risk Level: (Risk Level is High, Moderate, or Low)

Moderate

Ease-of-Fix: (Ease-of-Fix is Easy, Moderately Difficult, Very Difficult, or No Known Fix)

Easy

Estimated Work Effort: (Estimated Work Effort is Minimal, Moderate, Substantial, or Unknown; or a time estimate based on level of commitment and an adequate skill set)

Minimal

Description:

3.4.5 FFM 10112013

Finding

(b)(5)

This risk is mapped to row 7 from the initial collection spreadsheet.

(b)(5)

(b)(5)

(b)(5)

Recommended Corrective Action(s):

(b)(5)

3.4.6 **Business Risk**	(b)(5)

Applicable Standards:

NIST Security Control Families: Access Control (AC)

Reference: AC-7

Risk Level: (Risk Level is High, Moderate, or Low)

Low

Ease-of-Fix: (Ease-of-Fix is Easy, Moderately Difficult, Very Difficult, or No Known Fix)

Easy

Estimated Work Effort: (Estimated Work Effort is Minimal, Moderate, Substantial, or Unknown; or a time estimate based on level of commitment and an adequate skill set)

Minimal

Description:

3.4.6 FFM 10112013

Finding

(b)(5)

This risk is mapped to row 8 from the initial collection spreadsheet.

(b)(5)

(b)(5)

Recommended Corrective Action(s):

(b)(5)

4 DOCUMENTATION LISTS

The following tables list the documentation that MITRE requested prior to the onsite visit, as well as documentation provided to MITRE during and after the visit. The tables include the document element number, document title or information requested, and comments. Comments may include the name of the individual, organization, or agency that sent or delivered the documents and the date MITRE received the documents.

Table 5. Documentation Requested Prior to Onsite Visit

Document Element #	Document/Information Requested	Comments
D01	Information System Risk Assessment (ISRA)	G.Caulfield/ CGI Federal 08/12/2013 CALT doc43385
D02	System Security Plan (SSP) • SSP Workbook	G.Caulfield/ CGI Federal 08/12/2013 CALT doc42491 & doc42493
D03	Privacy Impact Assessment (PIA)	G.Caulfield/ CGI Federal 08/12/2013 CALT doc43900
D04	Contingency Plan	G.Caulfield/ CGI Federal 08/12/2013 CALT doc43901
D05	Uniformed Resource Locators (URL) to all Web application interfaces within assessment scope, if not documented in the SDD, VDD, or SSP	CGI Federal 09/16/2013
D06	System Design Document (SDD)	G.Caulfield/ CGI Federal 08/12/2013 CALT doc42632, doc42756, and doc38859
D07	Version Description Document (VDD)	G.Caulfield/ CGI Federal 08/12/2013 CALT doc42679, doc42727, and doc39345
D08	Interconnection agreements, Memorandum of Understanding (MOU) and/or Interconnection Security Agreement (ISA)	
D09	Rules of Behavior (RoB). Include evidence that RoBs have been acknowledged//signed by users	
D10	Contingency Plan Test	not completed as of 8/12/2013
D11	Configuration and change management process. Include examples of change requests (CR) from request to implementation in production	G.Caulfield/ CGI Federal 08/12/2013 CALT doc43904
D12	Baseline security configurations for each platform and the application within scope and baseline network configurations	G.Caulfield/ CGI Federal 08/12/2013 CALT doc43904
D13	Security Awareness and Training (AT) material. Include evidence of staff who have completed training	G.Caulfield/ CGI Federal 08/12/2013 CALT doc24409, doc24406, doc24407, and doc24405
D14	Incident Response (IR) procedures. Include evidence of simulations or actual execution of IR procedures	N/A, inherited control from PaaS
D15	Documentation describing the types of audit logging enabled and the established rules for log review and reporting	N/A, inherited control from XOC and Terremark

Document Element #	Document/Information Requested	Comments
D16	Open Corrective Action Plans (CAP) items from previous SCAs	G.Caulfield/ CGI Federal 08/12/2013 CALT doc44070
D17	System of Record Notice (SORN)	See the Master Health Insurance Exchange SORN 09-70-0560
D18	Operations & Maintenance (O&M) Manual	If databases and servers are in scope
D19	Application or system (depending on assessment's scope) backup and storage requirements and procedures. Include data retention and media handling/sanitization procedures	N/A
D20	Detailed system/network architecture diagrams with IP addresses of devices that will be within scope of assessment, if not documented in the SDD, VDD, or SSP)	May be documented in the SSP
D21	Security processes. Include application account creation and account review policy, password policy and malicious, mobile code, and antivirus policy. For password management, ensure policies cover both end user access as well as user accounts used for production operations	IN SSP
D22	CMS Security Certification Form (if system previously authorized—TAB A)	
D23	Technical Review Board (TRB) and TRA letters. Primarily for major updates and new applications	
D24	Administrator/Operator and User manuals or training materials, if not documented in the SDD, VDD, or SSP)	CGI Federal 09/16/2013

Table 6. Documentation Provided Prior to Onsite Visit

Document Element #	Document/Information Requested and Exchanged	Comments
D02	FFM SSP for August 2013 SCA.pdf	D. Lyles/CMS/ on 8/01/2013
D02	FFM SSP Workbook August 2013 SCA.pdf	D. Lyles/CMS/ on 8/01/2013
N/A	FFM HIX Aug 2013 SCA Scope as of 080713 Provided to CMS.docx	D. Lyles/CMS/ on 8/07/2013
D16	POAMs to Retest.docx	G.Caulfield/CGI Federal/ on 8/09/2013
D24	EE_R6.1.0_UserGuide.docx	ffmsca@cgifederal.com on /8/16/2013
D21	FFM_DirectEnrollmentAPI_Specifications.docx	ffmsca@cgifederal.com on /8/16/2013
D24	FM_R3_UserGuide.docx	ffmsca@cgifederal.com on /8/16/2013

Document Element #	Document/Information Requested and Exchanged	Comments
D06	PM_R5.3.0_SystemDesignDocument.docx	ffmsca@cgifederal.com on /8/16/2013
D24	PM_R6.1.0_PlanPreview_UserGuide.docx	ffmsca@cgifederal.com on /8/16/2013
D11	HIX Configuration Management Plan August 2013.docx	ffmsca@cgifederal.com on /8/16/2013
D01	HIX IS RA August 15 2013.docx	ffmsca@cgifederal.com on /8/16/2013
D11	HIX Configuration Management Plan August 2013.docx	ffmsca@cgifederal.com on /8/16/2013

Table 7. Documentation Received During Onsite Visit

Document Element #	Document/Information Received	Comments
D24	Connecting to CGI Herndon Wireless .doc	ffmsca@cgifederal.com on 8/19/2013
N/A	FFM HIX Aug 2013 SCA Scope.docx	ffmsca@cgifederal.com on 8/19/2013
D24	SCA Onsite Logistics.docx	ffmsca@cgifederal.com on 8/19/2013
N/A	ApplicationTestData_635_FFM.xlsx	ffmsca@cgifederal.com on 8/20/2013
N/A	DIRECT-ENROLLMENT_TESTING.pdf	ffmsca@cgifederal.com on 8/20/2013
D24	MITRE Aug2013 SCA guidance (test data, URLs, etc).docx	E. Quaintance/CGI Federal / on 8/20/2013
N/A	planpreview_testdata.xlsx	ffmsca@cgifederal.com on 8/20/2013
D21	FW Secure Code for Plan Compare.msg	M. Oh/CMS/ on 8/20/2013
D10	FFM CP Scenario Test Card 2.docx	ffmsca@cgifederal.com on 8/20/2013
D10	FFM-CP-Table Top Test_08162013_JK.docx	ffmsca@cgifederal.com on 8/20/2013
D04	HIX ISCP August 2013.docx	ffmsca@cgifederal.com on 8/20/2013
N/A	FFM Aug 2013 SCA Scope-Known_limitations.docx (CALT- doc47157)	ffmsca@cgifederal.com on 8/20/2013
D06	Plan Management System Design Document version 8.0 dated 030113.docx	ffmsca@cgifederal.com on 8/21/2013
D12	FFE PM-API CMS Issuer Gateway Interface Control Document version 2.0 dated 030113.docx	ffmsca@cgifederal.com on 8/21/2013
D11	CR Log Flow.vsd	ffmsca@cgifederal.com on 8/21/2013
D01	HIX IS RA June 2013.docx	ffmsca@cgifederal.com on 8/21/2013
D07	EE Release Notes.docx CALT (doc47327)	ffmsca@cgifederal.com on 8/21/2013
D07	FFE_R5_ReleaseNotes version 2.0 dated 030113.docx	ffmsca@cgifederal.com on 8/21/2013
D07	FM Release Notes.docx CALT (doc47329)	ffmsca@cgifederal.com on 8/21/2013

Document Element #	Document/Information Received	Comments
D24	Metal Level Description.docx CALT (doc47347).	ffmsca@cgifederal.com on 8/21/2013
D12	07.22.13.Hub.cms.gov.xss.docx (SecureZIP Attachments.zip)	D. Lyles/CMS/ on 8/22/2013
D12	(b)(5), (b)(6), (b)(7)c 2013-0228.docx CALT (doc47405)	ffmsca@cgifederal.com on 8/22/2013
D12	doc47381.txt CALT (doc47381)	ffmsca@cgifederal.com on 8/22/2013

CENTERS FOR MEDICARE & MEDICAID SERVICES

OFFICE OF INFORMATION SERVICES
7500 Security Boulevard
Baltimore, MD 21244-1850

Continued Health Information eXchange (HIX), August 2013 Security Controls Assessment Test Plan

September 17, 2013

FINAL

Table of Contents

List of Tables

1 INTRODUCTION

1.1 Purpose

This document describes the security controls assessment (SCA) methodology, schedule, and requirements that The MITRE Corporation (MITRE) will use to evaluate the Health Information eXchange (HIX) modules that were not tested previously. Specifically, the Plan Management(PM), Financial Management(FM) and the Enrollment and Eligibility (E&E) modules. The goal of the SCA test plan is to explain clearly the information MITRE expects to obtain prior to the assessment, the areas that will be examined, and the proposed scheduled activities MITRE expects to perform during the assessment. This document is meant to be used by the Centers for Medicare & Medicaid Services (CMS) and CGI Federal technical managers, network engineers, and system administrators responsible for system operations.

1.2 Security Controls Assessment Background

MITRE operates a federally funded research and development center (FFRDC) providing services to the government in accordance with the provisions and limitations defined in the Federal Acquisition Regulation (FAR) part 35.017. According to this regulation, in order for an FFRDC to discharge its responsibilities to the sponsoring agency, it must have access to government and supplier data (e.g., sensitive and proprietary data) and to employees and facilities beyond that which is common to the normal contractual relationship. As an FFRDC agent, MITRE is required to conduct its business in a manner befitting its special relationship with the government, to operate in the public interest with objectivity and independence, to be free from organizational conflicts of interest, and to have full disclosure of its affairs to the sponsoring agency.

MITRE is tasked by CMS to perform an application-only scope SCA in accordance with the *CMS Information Security (IS) Authorization to Operate Package Guide, v2.0*[1] for the HIX's available modules that have not previously undergone a Security Controls Assessment(SCA) located at the located at (b)(5), (b)(6), (b)(7)c, (b)(7)e (b)(5), (b)(6), (b)(7)c, (b)(7)e SCA complies with federal standards, policies, and procedures including the Federal Information Security Management Act of 2002 (FISMA) and the security-related areas as established and specified by the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Rev. 3, *Recommended Security Controls for Federal Information Systems and Organizations*[2] and the mandatory, non-waiverable Federal Information Processing Standards (FIPS) 200, *Minimum Security Requirements for Federal Information and Information Systems*.[3]

To comply with the federal standards, agencies must first determine the security category of their information system in accordance with the provisions of FIPS 199, *Standards for Security*

[1] http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/ATO_Package_Guide.pdf

[2] http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf.

[3] http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf.

Categorization of Federal Information and Information Systems,[4] and then apply the appropriate set of minimum (baseline) security controls in compliance with the NIST SP 800-53. Furthermore, CMS developed and published the *Information Security (IS) Acceptable Risk Safeguards (ARS) including CMS Minimum Security Requirements (CMSR) Version 1.5*,[5] *CMS Policy for Information Security Program (PISP)*,[6] and *Business Partners Systems Security Manual Version 10.0 (BPSSM)*.[7] The CMS ARS CMSR contains a broad set of required security standards based upon NIST SP 800-53 and NIST 800-63, *Electronic Authentication Guideline*[8] as well as additional standards based on CMS policies, procedures and guidance, other federal and non-federal guidance resources, and industry best practices. To protect CMS information and CMS information systems, the controls outlined in these policies must be implemented.

1.3 Assessment Process and Methodology

This section outlines MITRE's assessment methodology to verify and validate that the management, operational, and technical controls are appropriately implemented.

1.3.1 Phase 1: Planning

The first phase, "Planning", defines the assessment's scope, identifies goals, sets boundaries, and identifies assessment activities. This phase, as well as subsequent phases, requires the coordination of all involved parties, including CMS, MITRE, and CGI Federal. During this phase, the MITRE Evaluation Team will review all security policies and procedures in accordance with CMS security requirements as previously noted. The team will then create assessment scenarios and premises and define agreeable assessment terms as approved by CMS.

1.3.2 Phase 2: Assessment

Phase 2 may have several steps depending on the assessment's objectives, scope, and goals as set forth in the Planning Phase. These steps can be grouped by the nature of the activities involved. These activity groups are as follows:

- Information Collection—thorough research that must be performed against the target system/application before any meaningful assessment can be conducted. Data gathered is analyzed as the assessment proceeds and when the assessment is complete.
- Enumeration—activities that provide specific information about assessment targets. This information is often collected using appropriate software tools.
- Testing and Review—activities that typically involve both the automated testing of security vulnerabilities via software tools, manual analysis, and the evaluation of particular aspects of the organization's security policies and practices by the MITRE Evaluation Team members. MITRE's evaluation goal is to apply experience and insight in order to determine

[4] http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf.

[5] ARS CMSR Version 1.5 (July 31, 2012) at https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html.

[6] http://www.cms.hhs.gov/informationsecurity/downloads/PISP.pdf

[7] http://www.cms.gov/manuals/downloads/117_systems_security.pdf (July 17, 2009).

[8] http://csrc.nist.gov/publications/nistpubs/800-63-1/SP-800-63-1.pdf.

whether the system adequately implements security controls defined by CMS policies and standards.

1.3.3 Phase 3: Reporting

Phase 3, "Reporting", documents the soundness of the implemented security controls and consolidates all findings into the final output. This output includes reports that provide a summary of key findings and actionable recommendations, as well as provisions for all information derived from the assessment.

Depending on the results of these activities, it may be necessary to repeat appropriate phases. Throughout the entire process, the MITRE Evaluation Team will keep all involved parties informed of the progress and findings, as well as provide briefings of findings to CMS and CGI Federal staff. Evidence to support any weaknesses discovered will consist primarily of screen prints, script output, and session data. MITRE will immediately notify CMS and CGI Federal staff if significant or immediately exploitable vulnerabilities are discovered during the assessment.

2 PLANNING

This section contains information describing the modules, sometimes referred to as "applications", and environment that will be assessed, the scope of the assessment, any limitations, and roles and responsibilities of staff who will participate in the assessment.

2.1 Plan Management Background

Plan Management

The Plan Management (PM) Qualified Health Plan (QHP) Issuer Certification module of the Federally Facilitated Marketplace (FFM) is a means for the Issuers, States, and the Centers for Medicare and Medicaid Services (CMS) to enter data that can later be used for displaying the plans and benefits for consumers.

The PM business area consists of business processes for acquiring, certifying, monitoring, renewing, and managing the withdrawal of qualified health plans (QHPs) and the Issuers that offer these plans for a given Marketplace. These areas are currently supported by a composite solution consisting of:

- Data submission templates (MS Excel-based) allowing States and Issuers or their representatives to download, populate, validate, and upload into the PM system various complex data sets detailing application, plan, and rate and benefits information.
- User interfaces and services for State and Issuer users to submit, review, modify, and attest to the information uploaded or provided directly via the user interface to support the application and rate and benefits collection process for a given Exchange or set of Exchanges.
- User interfaces and services for CMS personnel to review, monitor, and certify/decertify applications and plans submitted for approval in a given Exchange.
- System interfaces to existing CMS systems (e.g., HIOS) to support streamlined data and profile collection and authentication.
- A system interface to CMS's PDF generation solution, Digi_Docs, based on Adobe LifeCycle, for creation of notices that are distributed to Issuers.

The Plan Preview module provides Issuers with the capability to view rates and plan details based on a set of subscriber and plan variance data selected by the user. The Summary page provides the user with the ability to select a specific IssuerID to preview their plan(s). The user can view an Issuer's submitted plans and rating scenarios by clicking on the View Plans button that corresponds to an Issuer in the Issuer table. The Rating Scenarios page allows the user to select plans and various inputs necessary for the rating engine to provide a rate(s).

2.2 Assessment Scope

MITRE is tasked with providing an application-only SCA to determine if the HIX updates have properly implemented CMS security standards. According to the System Security Plan (SSP), the FIPS 199 security categorization level for the HIX is Moderate since HIX contains sensitive information about persons and sensitive documents from insurance companies. The SCA will examine the management, operational, and technical controls that support the HIX updated modules listed below to ensure adherence to the Moderate security level specifications in the CMS ARS CMSR, PISP, and BPSS. To adequately perform the SCA, MITRE anticipates that the MITRE Evaluation Team will be onsite for five days from September 16-20, 2013.

Application testing will be performed in various environments, see chart below, and in adherence to the *CMS Information Security (IS) Assessment Procedure Version 2.0*[9] that establishes a uniform approach for the conduct of IS testing of the CMS Information Systems for major applications and their underlying component application systems. The following CMS ARS CMSR security control families will be the focus for testing:

Application Only Scope SCA:

- Access Control (AC), all controls except AC-1, AC-18, AC-19, and AC-20
- Awareness and Training (AT), only AT-2 and AT-3
- Audit and Accountability (AU), all controls except AU-1
- Security Assessment and Authorization (CA), all controls except CA-1
- Configuration Management (CM), all controls except CM-1
- Contingency Planning (CP), all controls except CP-1, CP-6, CP-7, CP-8, and CP-9
- Identification and Authentication (IA), all controls except IA-1, and IA-3
- Maintenance (MA), only MA-3
- Media Protection (MP), only MP-5 and MP-6
- Physical and Environmental (PE), only PE-2, PE-5, and PE-17
- Planning (PL), all controls except PL-1 and PL-4
- Personnel Security (PS), all controls except PS-1, PS-2, PS-3, and PS-8
- Risk Assessment (RA), only RA-2 and RA-3
- System and Services Acquisition (SA), all controls except SA-1, SA-7, and SA-9
- System Communications (SC), all controls except SC-1, SC-4, SC-12, SC-17, SC-20, SC-21, SC-22, and SC-32
- System and Information Integrity (SI), all controls except SI-1, SC-3, SI-5, and SI-8

[9] http://www.cms.hhs.gov/informationsecurity/downloads/Assessment_Procedure.pdf (March 19, 2009).

2.2.1 Modules to be tested by MITRE

Eligibility and Enrollment (E&E)

- Create Account
- Complete Application
- Eligibility Determination
- Plan Compare

2.2.2 Modules to be tested by Blue Canopy

Eligibility and Enrollment (E&E)

- Call Center
- Direct Enrollment
- Enrollment
- Notices & Mailing

Plan Management (PM)

- Plan Certification

2.2.3 Modules and functions not being tested

MODULE NAME	CAPABILITY	FUNCTIONALITY	AUGUST 2013 SCA CAPABILITY
E&E	Create account	My account - to do list	Link between my account & individual application
	Create account	My account - my profile	My account
	Create account	My account - account settings	My account
	Appeals	Link to appeals form	My account link to external link
	Plan compare	Screening questions	Plan compare
	Plan compare	Compose enrollment groups	Plan compare
	Plan compare	Plan results / plan filter / plan details	Plan compare

MODULE NAME	CAPABILITY	FUNCTIONALITY	AUGUST 2013 SCA CAPABILITY
	Plan compare	Compare plans / select plan (single tax household)	Plan compare
	Plan compare	Anonymous shopper	Plan compare
	Plan compare	Calculate max aptc	Plan compare
	Eligibility support	My account - identity proofing - ESD & account creation with ability to view eligibility and enrollment status	ESD
	Eligibility support	Eligibility support desktop - integration with serco	ESD
	Eligibility support	User interface / workflow / task queue	ESD
	Eligibility support	Document upload from my local folder	ESD
FM	SBM data collection	SBM data collection	SBM data collection
	CSR calculation - preliminary & final	CSR calculation - preliminary & final	CSR calculation - preliminary & final

2.2.4 Known Testing Limitations and Omissions

- Monday September 16, 2013 – Testing in (b)(5), (b)(6), (b)(7)c, (b)(7)e
- Tuesday September 17, 2013 through Friday September 20, 2013 – testing (b)(5), (b)(6), (b)(7)c, (b)(7)e from 8am to 4pm.
- Initial Enrollment and Change Enrollment (Cancel / Terminate) – Cancel and Terminate Enrollment is developed and undergoing unit testing. This will not be available for testing until the new enrollment service move (b)(5), (b)(6), (b)(7)c, (b)(7)e argeting to complete unit testing by COB 9/16.
- Process Inbound 834s from Issuers (Effectuation, Cancellations, Terminations) – We need to create files (coordinate with HUB) for processing any inbound transactions.
- Transaction Logging (999, 834, Business Acknowledgement) – (b)(5) (b)(5)

2.3 Assessment Assumptions/Limitations

MITRE has identified limitations of the planned assessment:

- The (b)(5), (b)(6), (b)(7)c, (b)(7)e databases are out of scope.
- Policies, Procedures, Operating Systems images (b)(5), (b)(6), (b)(7)c, (b)(7)e (b)(5), (b)(6), (b)(7)c, (b)(7)e scope.
- (b)(5), (b)(6), (b)(7)c, (b)(7)e and all their services are out of scope.
- The application modules being tested is functionally equivalent to the application deployed in the production environment.
- CGI Federal staff will provide timely responses to MITRE requests for information, access to systems to perform application testing and CGI Federal subject matter experts as documented in the SCA test plan.
- All the policies and procedure that govern the testable modules are the same policies and procedures that were assessed as part of the HIX/QHP assessment March-April 2013.
- Findings remediation for previously assessed modules (Operating System, Database and Applications) are considered to be secondary and may be reevaluated if time and resources permit..
- Code Changes, hot fixes, patches etc. will be made known to MITRE via email PRIOR to the change being performed, followed by the documented authorization for the change, which states what the change was and who authorized it.
- Test Data will be prepopulated by CGI Federal for some test accounts.
- No application interviews will be formally scheduled. Ad-Hoc application interviews may be performed as needed and agreed upon by MITRE and CGI Federal.

2.4 Data Use Agreement

The Data Use Agreement (DUA), form CMS-R-0235, must be executed prior to the disclosure of data from the CMS Systems of Records to ensure that the disclosure will comply with the requirements of the Privacy Act, Privacy Rule, and CMS data release policies. It must be completed prior to the release of, or access to, specified data files containing protected health information (PHI) and individual identifiers. MITRE has completed and signed this agreement with CMS Reference DUA number 19317; expiration date August 27, 2014.

2.5 Roles and Responsibilities

To prepare for the assessment, the organization(s) and MITRE will identify personnel associated with specific responsibilities. Individuals may have responsibilities that span multiple roles or have knowledge pertaining to the implementation of more than one security control area. This section provides a description of the roles and responsibilities to assist the organization(s) and MITRE in determining the appropriate personnel who should be available for the assessment.

2.5.1 Application Developer/Maintainer

The Application Developer/Maintainer shall have a thorough knowledge of the application security control requirements for the system and their implementation to protect the software application, its data in transit and at rest, as well as the implementation and configuration standards utilized by the organization. These controls may include access control, audit and accountability, user identification and authentication, software code configuration control, application integrity, and communications protection. During the SCA process and onsite assessment, the Application Developer/Maintainer shall be available for planning sessions, interviews, application discussions, providing assistance for using the application, providing documentation under their control, and remediating any weaknesses.

2.5.2 Business Owner

The Business Owner is responsible for the successful operation of the system and ultimately accountable for system security. The Business Owner defines the system's functional requirements, ensures that Security Accreditation (previously referred to as Certification and Accreditation [C&A]) activities are completed, maintains and reports on the Plan of Action & Milestones (POA&M), and ensures that resources necessary for a smooth assessment are made available to the MITRE Evaluation Team (Assessment Contractor). During the SCA process and onsite assessment, the Business Owner shall be available for planning sessions, interviews, system discussions, providing documentation, and providing assistance when necessary (access, contacts, decisions, etc.) In some cases the Business Owner may be the System Owner.

2.5.3 CMS Facilitator

The CMS Facilitator is a member of the CMS SCA Team staff responsible for scheduling and communicating information on all planning and coordinating meetings as well as out-briefs associated with the SCA. The CMS Facilitator reserves work space for testing when the tests are conducted at CMS facilities. In addition, the CMS Facilitator coordinates the logistics between the CMS SCA Team and SCA Stakeholders (application developers, maintainers, technical support, business owners, etc.) The CMS Facilitator is responsible for initiating application and system access for the test accounts used during the assessment. At the conclusion of the assessment, the CMS Facilitator accepts the Security Controls Assessment Report, distributes the final report to SCA Shareholders and generates the cover letter associated with it.

2.5.4 CMS Government Task Lead

The CMS Government Task Lead (GTL) is a CMS representative for the Application Developer/ Maintainer and is responsible for providing technical information to the SCA Team. During the SCA process and onsite assessment, the GTL shall be available for planning sessions, interview with their Application Developer/ Maintainer, assisting the Application Developer during application discussions, providing assistance for using the application, and directing the Application Developer/Maintainer to remediate any weaknesses.

2.5.5 Information System Security Officer or System Security Officer

The Information System Security Officer (ISSO) or System Security Officer (SSO) is responsible for ensuring that the management, operational, and technical controls to secure the system are in place and effective. The ISSO shall have knowledge of the following:

  - All controls implemented or planned for the system
  - Security audit controls and evidence that audit reviews occur
- System Security Plan (SSP) and any authorized exceptions to security control implementations

The ISSO shall be responsible for all security aspects of the system from its inception until disposal. During the SCA process and onsite assessment, the ISSO plays an active role and partners with the CMS Facilitator to ensure a successful SCA. The ISSO shall be available for interview, provide or coordinate the timely delivery of all required SCA documentation; and coordinate and schedule interviews between the SCA Team and SCA Stakeholders. The ISSO is designated in writing and must be a CMS employee.

2.5.6 Lead Evaluator

The Lead Evaluator is a member of the MITRE Evaluation Team and responsible for understanding CMS policies, standards, procedures, system architecture and structures. The Lead Evaluator has limited activities within the SCA scope; reports all vulnerabilities that may impact the overall security posture of the system; refrains from conducting any assessment activities that she/he is not competent to carry out or to perform in a manner which may compromise the information system being assessed; and coordinates getting information, documentation and/or issues addressed between the MITRE Evaluation Team, the CMS Facilitator, and the SCA Stakeholders. The Lead Evaluator must develop the *Assessment Plan;* modify the testing approach, when necessary according to the scope of the assessment; prepare the daily agenda, preliminary findings worksheets and conduct the Onsite Assessment briefings; and prepare a Security Controls Assessment Report (e.g., Findings Report) to communicate how the CMS business mission will be impacted if an identified vulnerability is exploited.

2.5.7 Program Manager

The Program Manager shall have a high-level understanding of the assessed system, as well as the ability to describe organizational and system policies from an enterprise perspective, with which the system shall be in compliance. The Program Manager shall be familiar with access controls, both physical and logical, contingency plans (i.e., alternate sites/storage, system restoration and reconstitution), user identification and authentication, system authorization to operate, incident response, resource planning, system and software acquisition, flaw remediation, and system interconnections and monitoring. During the SCA process and onsite assessment, the Program Manager shall be available for interview and to provide documentation that falls under the Program Manager’s responsibility.

2.5.8 System Owner

The System Owner is responsible for the successful operation of the system and accountable for system security. The System Owner is also responsible for executing crucial steps to implement management and operational controls and to ensure that effective technical controls are implemented to protect the system and its data. The System Owner formally designates the ISSO. In conjunction with the Business Owner, the System Owner is responsible for ensuring that Security Accreditation activities are completed and the POA&M is maintained and reported. During the SCA process and onsite assessment, the System Owner shall be available for interview and, with the assistance of the system’s support staff, ensure that all documentation required for the assessment is available to the SCA Evaluator. The System Owner may be the Business Owner.

2.6 Assessment Responsibility Assignment

For this assessment, MITRE, CMS, and CGI Federal staff names have been associated with the specific roles and corresponding responsibilities. The Business Owner may delegate their responsibilities during the engagement, but the name of the delegated individual should be updated in Table 1, which provides details on the responsibilities for the assessment based on the identified roles and responsibilities provided in the preceding Section, “Roles and Responsibilities.”

Table 1. Assessment Responsibilities

Name	Organization	Role
Kirk Grothe	CMS/OIS/CIISG	Application Developer
Jim Kerr	CMS/OIS/CIISG	Business Owner
Darrin Lyles	CMS/OIS/CIISG	CMS Facilitator (Lead)
Mark Oh	CMS/OIS/CIISG	CMS Government Task Leader
Joe (Zhengyu) Zhu	CGI Federal	Database Administrator
Tom Schankweiler Darrin Lyles	CMS/OIS CMS/OIS	SSO ISSO
Jim Bielski	MITRE	Project Lead
Jim Huff	MITRE	Lead Evaluator
Mark Calem	CGI Federal	Project Manager
Monica Winthrop	CGI Federal	Deputy Project Manager
Patrick Bruszewski	CGI Federal	System /(b)(5), (b)(6), (b)(7)c, (b)(7)e
Rich McCoy	CGI Federal	Plan Management Release Manager
Keith Rubin	CGI Federal	Chief Architect
Balaji Ramamoorthy	CGI Federal	Senior Security Architect
Raj Sundar	CGI Federal	Security Architect
Joel Singer	CGI Federal	Infrastructure Manager
Patrick Bruszewski	CGI Federal	Infrastructure Configuration Manager
Patrick Bruszewski	CGI Federal	Infrastructure Engineer

2.7 Physical Access and Work Area Requirements

MITRE will require access to various systems, networks, infrastructure, and facilities. The MITRE Evaluation Team will require direct network connectivity to CGI Federal servers and also network access to the Internet. A work area for these individuals needs to be established and include power, table, and chairs. In addition, MITRE staff will require a work area for conducting interviews and analyzing data. CGI Federal will reserve appropriate facilities for the MITRE Evaluation Team while onsite at (b)(5), (b)(6), (b)(7)c, (b)(7)e

.

3 ASSESSMENT

This section contains information describing the activities to be performed during the assessment for information collection, enumeration, testing and review.

3.1 Information Collection

MITRE will require access to documentation, operating system and network configuration data, and application information in order to begin the assessment.

3.1.1 CMS FISMA Controls Tracking System (CFACTS) Name

To ensure that the final security controls/ findings worksheet can be properly loaded in to the CMS FISMA Controls Tracking System (CFACTS) at the end of the assessment MITRE must have the correct system name as contained within CFACTS. This system name will be used to correctly populate the System Name field in the Final Management Worksheet delivered with the Final Report.

CFACTS System Name
FFM
Prior to September 2013, the CFACTS name was "HIX"

3.1.2 Documentation Requirements

MITRE must obtain the documentation requested one week prior to the onsite Assessment "Kick-off" meeting. In order to effectively perform the assessment and prevent delays during the SCA, MITRE must receive the following information that pertains to the application and/or system under evaluation prior to arriving onsite. Failure to receive this information in a timely manner will impact the assessment's quality and MITRE's ability to determine whether management, operational, and technical controls have been implemented properly. To assist MITRE in determining the completeness of this information and serve as a checklist, CMS and CGI Federal should use Tables 2–5 as guides and include any comments that may be applicable (e.g., new system being accredited, no SSP Accreditation Form provided, Configuration Management Plan included in SSP, server Internet Protocol (IP) addresses, and network diagram included in the System Design Document [SDD]). The documentation is broken into four categories:

- Mandatory Pre-Assessment Documentation
- Documentation Required by Policy (e.g., PISP or Integrated IT Investment and System Life Cycle Framework [Integrated Life Cycle (ILC) Framework])
- Expected/Supporting Documentation
- Additional Documentation

Mandatory Pre-Assessment Documentation: The documents in Table 2. Mandatory Pre-Assessment Documentation should be provided within a week after the preliminary call (or within the agreed upon timeframes as noted in the preliminary call meeting minutes) for use in the development of the draft test plan. These can be draft documents if necessary, but "final versions" must be provided at least one week prior to the on-site assessment. Failure to receive these documents could affect the quality of the assessment and would be an ineffective and inefficient use of funds for the assessment to continue. Starting in August, 2012, there may also be additional funding required before the onsite testing can proceed if all requirements are not addressed prior to the scheduled testing date. However, there may be special cases in which CMS wants the evaluator to proceed without all of the documentation, such as a FISMA one-third SCA or if CMS believes a project/system/application is placing CMS at such a great risk that funding may be pulled. For the latter, CMS will request the evaluator's advice on the risk that is posed.

Table 2. Mandatory Pre-Assessment Documentation

Document Element #	Document/Information Requested	ARS CMSR	Policy	Comments
D01	Information System Risk Assessment (IS RA)	RA-3 Risk Assessment	ILC Framework CMS PISP CMSR	G.Cauldfield/ CGI Federal 09/09/2013 CALT doc50840
D02	System Security Plan (SSP) SSP Workbook	PL-2 System Security Plan CA-4 Security Certification	ILC Framework CMS PISP FISMA CMSR	G.Cauldfield/ CGI Federal 09/09/2013 CALT doc50842 & doc50843
D03	Privacy Impact Assessment (PIA)	PL-5 Privacy Impact Assessment	ILC Framework CMSR	G.Cauldfield/ CGI Federal 09/09/2013 CALT doc50841
D04	Contingency Plan	CP-2 Contingency Plan	ILC Framework CMSR	G.Cauldfield/ CGI Federal 09/09/2013 CALT doc50837
D05	**Uniformed Resource Locators (URL) to all Web application interfaces within scope of assessment, if not documented in the SDD, VDD, or SSP)**	SA-5 Information System Documentation	CMSR	

Documentation Required by Policy: CMS Policy requires that a system or application have the following documents listed in Table 3. The absence of these documents is handled in a uniform manner. For example, if policy requires document D12, Baseline Security Configurations, be completed and it does not exist, the absence of the document will result in a finding, assuming the security control is in scope for the assessment.

Table 3. Documentation Required by Policy

Document Element #	Document/Information Requested	ARS CMSR	Policy	Comments
D06	**System Design Document (SDD)**	SA-3 Life Cycle Support	ILC Framework CMSR	G.Cauldfield/ CGI Federal 08/12/2013 CALT doc42632, doc42756, and doc38859
D07	**Version Description Document (VDD)**	SA-3 Life Cycle Support	ILC Framework	G.Cauldfield/ CGI Federal 08/12/2013

Document Element #	Document/Information Requested	ARS CMSR	Policy	Comments
			CMSR	CALT doc42679, doc42727, and doc39345
D08	Interconnection agreements, Memorandum of Understanding (MOU) and/or Interconnection Security Agreement (ISA)	CA-3 Information System Connections SA-9 External Information System Services	CMSR	
D09	RoB. Included evidence that RoBs have been acknowledged//signed by users	PL-4 Rules of Behavior	CMSR	
D10	Contingency Plan Test	CP-4 Contingency Plan Testing and Exercises	ILC Framework CMSR	G.Cauldfield/ CGI Federal 09/09/2013 CALT doc48045
D11	Configuration and change management process. Include examples of change requests (CR) from request to implementation in production	CM-3 Configuration Change Control CM-4 Monitoring Configuration Changes CM-5 Access Restrictions for Change	CMSR	G.Cauldfield/ CGI Federal 08/12/2013 CALT doc43904
D12	**Baseline security configurations for each platform and the application within scope and baseline network configurations**	CM-2 Baseline Configuration CM-6 Configuration Settings	CMSR	G.Cauldfield/ CGI Federal 08/12/2013 CALT doc43904
D13	Security awareness and training (AT) material including evidence of staff who have completed training	AT-1 Security Awareness and Training Policy and Procedures AT-2 Security Awareness AT-3 Security Training AT-4 Security Training Records AT-5 Contacts with Security Groups and Associations	CMSR	G.Cauldfield/ CGI Federal 08/12/2013 CALT doc24409, doc24406, doc24407, and doc24405
D14	Incident response (IR) procedures. Include evidence of simulations or actual execution of IR procedures	IR-1 Incident Response Policy and Procedures IR- 2 Incident Response Training IR- 3 Incident Response Testing and Exercises IR- 4 Incident Handling IR- 5 Incident Monitoring IR- 6 Incident Reporting IR- 7 Incident Response Assistance	CMSR	N/A, inherited control from PaaS
D15	**Documentation describing the types of audit logging that is enabled and the established rules for log review and reporting**	AU-6 Audit Monitoring, Analysis, and Reporting	CMSR	N/A, inherited control from XOC and Terremark

Document Element #	Document/Information Requested	ARS CMSR	Policy	Comments
D16	Open Corrective Action Plans (CAP) items from previous security controls assessments	CA-5 Plan of Action and Milestones (POA&M)	CMSR	G.Cauldfield/ CGI Federal 08/12/2013 CALT doc44070
D17	System of Record Notice (SORN)	PL-5	ILC Framework CMSR	See the Master Helath Insurance Exchange SORN 09-70-0560

Expected/Supporting Documentation: Table 4 provides a list of other supporting documents that are applicable to an application or system. Although these documents are not specifically required by security policy, the documents should exist based on the CMS ILC and should be provided to MITRE during the assessment as they may be helpful in performing the assessment, determining any special circumstances or permissions that vary from the CMS standards and also used as substantiating artifacts.

Table 4. Expected/Supporting Documentation

Document Element #	Document/Information Requested	ARS CMSR	Policy	Comments
D18	**Operations & Maintenance (O&M) Manual**	SA-5 Information System Documentation	ILC Framework CMSR	If databases and servers are in scope
D19	Application or system (depending on assessment's scope) backup and storage requirements and procedures. In addition, include data retention and media handling/sanitization procedures	CP-6 Alternate Storage Site CP-9 Information System Backup MP-4 Media Storage MP-6 Media Sanitization and Disposal	CMSR	N/A
D20	Detailed system/network architecture diagrams with IP addresses of devices that will be within scope of assessment, if not documented in the SDD, VDD, or SSP)	SA-5 Information System Documentation	CMSR	May be documented in the SSP
D21	Security *processes*, including application account creation and account review policy, password policy and malicious, mobile code, and antivirus policy. For password management, ensure policies cover both end user access as well as user accounts used for production operations	AC-1 Access Control Policy and Procedures IA-1 Identification and Authentication Policy and Procedures	CMSR	IN SSP
D22	CMS Security Certification Form (if system previously authorized—TAB A)	CA-6 Security Authorization	CMSR	N/A

Document Element #	Document/Information Requested	ARS CMSR	Policy	Comments
D23	Technical Review Board (TRB) and TRA letters to include all PDR, DDR and ORR documentation. Primarily for major updates and new applications	CM-3 Configuration Change Control	CMSR	Required to determine variances from the CMS Policies and Standards

Additional Documentation: Additional documentation in Table 5 may be requested during the assessment, depending on the system/application being assessed.

Table 5. Additional Documentation

Document Element #	Document/Information Requested	ARS CMSR	Policy	Comments
D24	**Administrator/Operator and User manuals or training materials, if not documented in the SDD, VDD, or SSP)**	SA-5 Information System Documentation	ILC Framework CMSR	Application Walkthrough and supplemental documentation to assist understanding of PM Module testing.

3.1.3 Application Testing Requirements

In order to test the HIX Module applications, accounts that reflect the different user types and roles need to be created and tested prior to MITRE arriving onsite. MITRE requires that application-specific user accounts be created for MITRE Evaluation Team members as authorized by CMS. This will enable MITRE to test application security controls and environment vulnerabilities.

The document "*FFM SCA TestData Sept 2013 v2.docx*" provided by CGI Federal on Tuesday September 17, 2013 contains URLS, username, passwords and test case information.

3.2 Enumeration

MITRE will use various methods and tools to enumerate the system and it security policies.

3.2.1 Vulnerability Assessment Tools

MITRE will work with CMS and CGI Federal staff to verify and determine that industry standard best practices are reflected in the CMS system architecture design. To the extent possible, the work performed on this task will be accomplished on MITRE-furnished auditing equipment. The MITRE Evaluation Team may use the following tools during the assessment:

- **Achilles** (http://www.mavensecurity.com/achilles)—tool designed for testing the security of Web applications
- **Burp Suite** (http://portswigger.net/burp/)—integrated platform for performing security testing of web applications.

- **Cookie Digger** (http://www.foundstone.com)—tool used to collect and analyze cookie values used to maintain session state and isolation through identifying the use of easily guessed or predictable cookie values
- **Curl** (http://curl.haxx.se/)—open-source command line tool for transferring files with Uniformed Resource Locator (URL) syntax
- **Httprint** (http://net-square.com/httprint/)—Web server fingerprinting tool
- **Httrack** (http://www.httrack.com/)—open-source offline browser utility
- **MetaCoretex** (http://sourceforge.net/projects/metacorete (b)(5), (b)(6), (b)(7)c, (b)(7)e rovides a graphical user interface (GUI) and tests a number of different database systems
- **MITRE host-based and database scripts**—scripts developed with the contribution and experience of MITRE's vulnerability and penetration testers. Versions have been developed for both Windows and Unix-based operating systems. With the assistance of System Administrators, the MITRE Evaluation Team uses these scripts to audit operating system security configurations and identify misconfigurations
- **Mozilla and Firefox Web Browsers** (http://www.mozilla.org)—open-source Web-based browsers used to manually browse and inspect the Web application and associated forms
- **Nikto** (http://www.cirt.net/code/nikto.shtml)—open-source, command-line, Web server scanner
- **Nipper Studio (**https://www.titania-security.com/)— software tool that provides comprehensive security auditing and device configuration reporting of network devices, including firewall rule audits and software version vulnerabilities
- **Nmap** (http://www.insecure.org/nmap/)—open-source utility for network exploration or security auditing through UDP and TCP port scanning
- **Paros** (http://www.parosproxy.org) (b)(5), (b)(6), (b)(7)c, (b)(7)e used to evaluate Web application security (similar to Achilles)
- **Openssl** (http://www.openssl.org/)—open-source library that provides cryptographic functionality to applications such as secure Web servers
- **SiteDigger** (http://www.foundstone.com/)—tool that searches Google's cache to look for vulnerabilities, errors, configuration issues, proprietary information, and interesting security nuggets on websites
- **SpikeProxy** (http://www.immunitysec.com/resources-freesoftware.shtml)—Web proxy that captures and replays Hyper Text Transfer Protocol (HTTP) packets with permuted input
- **Stompy** (http://lcamtuf.coredump.cx)—open-source command line tool (b)(5), (b)(6), (b)(7)c, (b)(7)e used to collect and analyze cookie and URL parameter values used as session identifiers
- **Stunnel** (http://www.stunnel.org)—universal SSL wrapper that allows the encryption of arbitrary TCP connections inside SSL
- **WebScarab** (http://www.owasp.org/index.php/Category:OWASP_WebScarab_Project)— (b)(5), (b)(6), (b)(7)c, (b)(7)e used to evaluate Web application security

- **Wget** (http://www.gnu.org/software/wget/wget.html)—open-source network tool that retrieves files from the Internet using HTTP, Secure Hyper Text Transfer Protocol (HTTPS), and FTP protocols
- **Wireshark** (http://www.wireshark.org) – open source, GUI network protocol analyzer

The list above is not all inclusive. MITRE may use other tools and scripts, as needed, and provide test scripts to CMS to share with necessary support staff.

3.3 Testing and Review

MITRE will perform activities that typically involve both the automated testing of security vulnerabilities via software tools, manual analysis, and the evaluation of particular aspects of the organization's security policies and practices.

MITRE will perform the following assessment activities:

- Conduct vulnerability testing with full knowledge of the system, applications, products, configurations, and topology
- Provide MITRE Evaluation Team members, who have specific knowledge of operating systems, firewalls, networking, architecture of transactional Web systems, and Web programming technologies (e.g., Hypertext Markup Language [HTML], (b)(5), (b)(6), (b)(7)c, (b)(7)e Active Server Pages [ASP], cookies, Perl, Common Gateway Interface [CGI], Siebel, WebSphere, and Visual Basic scripting)
- Attempt to gain unauthorized user access or unauthorized access to system resources
- Evaluation of Web application buffer overflow and password vulnerabilities by performing tests that include brute force password attacks and buffer overflow
- Perform application testing to determine if adequate security controls are implemented
- Examine database configuration settings

3.3.1 Interviews

Interviews will focus on a review of the management, operational, and technical controls associated with the CMSR security policies, procedures, and standards. Interviews will also help gain a better understanding of the system environment's security posture and will supplement findings identified during the technical testing. When available and applicable, electronic copies of additional written documentation will be collected for review. Subject matter experts (SME) in the following areas will be interviewed:

- Application Testing

3.3.2 Application Testing

MITRE will test the HIX Modules to ensure proper software development techniques, supported software is used, and that the confidentiality, integrity and availability (CIA) of data processed by the application adhere to CMS policies, procedures and standards. Following is a list of activities MITRE will perform:

- Assess if input parameters passed to the application are checked and validated

- Determine if application administrators can remotely access the application via CMS-approved standards
- Examine implemented access control and identification and authentication techniques
- Test to determine if the application is susceptible to (b)(5), (b)(6), (b)(7)c, (b)(7)e (b)(5), (b)(6), (b)(7)c, (b)(7)e or other vulnerabilities
- Examine confidential information to determine if it is encrypted before being passed between the application and browser
- Determine if the application architecture conforms to the TRA

CMS and CGI Federal will provide the appropriate user accounts and logins to access the application to be tested in the targeted environment. The user account logins and application access must be available to MITRE for tests two weeks prior to application testing. At least one account must have administrative access with the ability to adjust the application roles of another login.

4 REPORTING

This section outlines how MITRE will report vulnerabilities during the assessment.

4.1 Security Controls Assessment Findings Spreadsheet

The SCA findings spreadsheet (Table8) is a running tabulation of possible findings identified during the assessment that is reviewed during daily out-briefs (DOB). Findings are broken out by day and then sorted according to risk level. For updates to a previous day's findings, the updated cell is highlighted in yellow. Although high and moderate risk-level findings are discussed during the DOBs, questions pertaining to low risk-level findings may be raised for clarification. Further details about the spreadsheet columns are listed in the following sections.

(b)(5), (b)(6), (b)(7)c, (b)(7)e

[redacted]

4.1.1 Row Number

Each finding has a row number included to provide easy reference when the spreadsheet is printed and reviewed during DOBs. This row number is also included in the test reports for easy cross reference.

4.1.2 Weakness

A brief description of the security vulnerability is described in the Weakness column.

4.1.3 Risk Level

Each finding is categorized as a business risk and assigned a risk level rating described as high, moderate, or low risk. The rating is, in actuality, an assessment of the priority with which each vulnerability should be addressed. Based on CMS' current implementation of the underlying technology and the assessment guidelines contained with the *CMS Reporting Procedure for Information System (IS) Assessments* document,[10] MITRE will assign these values to each Business Risk. The risk ratings are described in Table9.

Table 7. Risk Definitions

Rating	Definition of Risk Rating
High	Exploitation of the technical or procedural vulnerability will cause substantial harm to CMS business processes. Significant political, financial, and legal damage is likely to result
Moderate	Exploitation of the technical or procedural vulnerability will significantly impact the confidentiality, integrity and/or availability of the system or data. Exploitation of the vulnerability may cause moderate financial loss or public embarrassment to CMS
Low	Exploitation of the technical or procedural vulnerability will cause minimal impact to CMS operations. The confidentiality, integrity and availability of sensitive information are not at risk of compromise. Exploitation of the vulnerability may cause slight financial loss or public embarrassment
Informational	An "Informational" finding, is a risk that has been identified during this assessment which is reassigned to another major application (MA) or General Support System (GSS). The finding must already exist and be open for the reassigned MA or GSS. The informational finding will be noted in a separate section in the final SCA report, but will not be the responsibility of the assessed application to create a Corrective Action Plan, as it is reassigned to the MA or GSS.

4.1.4 CMSR Security Control Family and Reference

The CMSR security control family and control number that is affected by the vulnerability is identified in the CMSR Security Control Family and the Reference columns.

4.1.5 Affected Systems

The systems, URLs, IP addresses, etc., affected by the weakness, are identified in the Affected Systems column.

4.1.6 Ease-of-Fix

[10] http://www.cms.hhs.gov/informationsecurity/downloads/Assessment_Rpting_Procedure.pdf.

Each finding is assigned an Ease-of-Fix rating described as Easy, Moderately Difficult, Very Difficult, or No Known Fix. The ease with which the Business Risk can be reduced or eliminated is described using the guidelines in Table 80.

Table 8. Definition of Ease-of-Fix Rating

Rating	Definition of Ease-of-Fix Rating
Easy	The corrective action(s) can be completed quickly with minimal resources and without causing disruption to the system or data
Moderately Difficult	Remediation efforts will likely cause a noticeable service disruption: • A vendor patch or major configuration change may be required to close the vulnerability • An upgrade to a different version of the software may be required to address the impact severity • The system may require a reconfiguration to mitigate the threat exposure • Corrective action may require construction or significant alterations to the manner in which business is undertaken
Very Difficult	The high risk of substantial service disruption makes it impractical to complete the corrective action for mission critical systems without careful scheduling: • An obscure, hard-to-find vendor patch may be required to close the vulnerability • Significant, time-consuming configuration changes may be required to address the threat exposure or impact severity • Corrective action requires major construction or redesign of an entire business process
No Known Fix	No known solution to the problem currently exists. The Risk may require the Business Owner to: • Discontinue use of the software or protocol • Isolate the information system within the enterprise, thereby eliminating reliance on the system In some cases, the vulnerability is due to a design-level flaw that cannot be resolved through the application of vendor patches or the reconfiguration of the system. If the system is critical and must be used to support on-going business functions, no less than quarterly monitoring shall be conducted by the Business Owner, and reviewed by CMS IS Management to validate that security incidents have not occurred

4.1.7 Estimated Work Effort

Each finding has been assigned an Estimated Work Effort rating described as Minimal, Moderate, Substantial, or Unknown. The estimated time commitment required for CMS or contractor personnel to implement a fix for the Business Risk is categorized in Table 1.

Table 9. Definition of Estimated Work Effort Rating

Rating	Definition of Estimated Work Effort Rating
Minimal	A limited investment of time (i.e., roughly three days or less) is required of a single individual to complete the corrective action(s)
Moderate	A moderate time commitment, up to several weeks, is required of multiple personnel to complete all corrective actions
Substantial	A significant time commitment, up to several months, is required of multiple personnel to complete all corrective actions. Substantial work efforts include the redesign and implementation of CMS network architecture and the implementation of new software, with associated documentation, testing, and training, across multiple CMS organizational units
Unknown	The time necessary to reduce or eliminate the vulnerability is currently unknown

4.1.8 Finding

(b)(5)

(b)(5)

4.1.11 Recommended Corrective Actions

(b)(5)

(b)(5)

4.2 Reassignment of Findings

If during the SCA onsite testing period, a finding is determined to be outside the scope of the system or the responsibility of the CMS System Business Owner and ISSO, the finding will be reported and steps should be taken to reassign the finding to the rightful owner. The CMS SCA Facilitator will attempt to contact the rightful owner, provide them with the appropriate information, and invite them to the balance of the SCA proceedings. During the onsite week, the CMS facilitator may assist the CMS System Business Owner and ISSO to obtain the rightful owner's concurrence and responsibility for the finding.

However, it is ultimately the responsibility of the CMS System Business Owner and ISSO to obtain concurrence of the potential finding from the rightful owner and follow through with the necessary reassignment steps prior to the Draft Report Review. If the finding has already been reported in CFACTS, the System Business Owner and ISSO must obtain the CFACTS identifier from the rightful owner and the finding will be closed in the report noting the re-assignment and CFACTS information in the status field. If the ownership of the finding has not yet been successfully re-assigned by the time of the Draft Report Review, the report will be finalized with the finding assigned to the system. It is then the responsibility of the CMS System Business Owner and ISSO to address at a later time and update CFACTS accordingly with the proper information.

Once a finding is reassigned, it should be documented in the system's risk assessment (ISRA). The CMS System Business Owner and ISSO should review periodically as the finding may directly impact the system.

4.3 Reporting Observations

MITRE will include in the finding spreadsheet items that are considered observations instead of actual findings. An observation may arise as a result of a number of situations:

- A security policy or document may be changing and serves to inform the system owner. This gives ample time to prepare for and make appropriate changes;
- A security policy or document has changed and CMS has granted a grace period for completion. The observation provides a mechanism to the business owner/ ISSO that the item requires attention before the end of that grace period;
- A possible finding that the Security Assessment Contractor may have observed and cannot verify by testing as part of the existing tasking; or
- Issues related to industry "best practices" and that are not identified in the CMS Acceptable Risk Safeguards (ARS) or other guidelines referenced by the ARS. These items are considered "Opportunities for Improvement" (OFI).

The observations will also be included in the SCA report in a separate section. Observations may or may not require additional action of the part of the CMS Business Owner, ISSO or CGI Federal.

4.4 Reporting of (b)(5), (b)(6), (b)(7)c, (b)(7)e Vulnerabilities

(b)(5)

4.5 Test Reporting

MITRE will also conduct a final out-brief, if needed, after the onsite assessment is completed. Typically, MITRE does not have the opportunity to review all the documentation, configurations, and script outputs while onsite and will need additional days to finish identifying potential vulnerabilities. If this is the case, CMS will schedule a final out-brief within one week after the onsite assessment is completed.

MITRE will discuss and review all informational evidence of remediated findings that is supplied by CMS, and CGI Federal. The MITRE Evaluation Team will diligently respond to inquiries made by CMS, and CGI Federal concerning the validity of findings and acknowledge any areas of concern that may occur. The substance of evidence will contain any mitigation proof reflective of, and as close to, the source of the impacted system as possible. The manner of evidence exchange will be tracked and protected by the MITRE Team Lead, GTL, CMS

Facilitator and authorized Points of Contact (POC) for the system(s) tested. ***If CMS authorizes the submission of remediation evidence after the onsite dates, the focus should be on addressing High and Moderate risk findings. In order to promptly meet schedules, MITRE requests that all evidence of remediated findings be submitted to MITRE by the due date established by CMS. This is typically one week after the final out-brief.***

Approximately three weeks following the final out brief, MITRE will provide a draft test report. The test report takes the vulnerabilities identified in the findings spreadsheet and reformats and sorts the information to conform to CMS guidelines contained within the *CMS Reporting Procedure for IS Assessments* document. CMS and CGI Federal will be provided approximately one week to review the test report. Following a draft test report review conference call that will be scheduled by CMS, MITRE will generate a final test report and a data worksheet. The data worksheet will contain all findings not closed during the onsite or the remediation period following the assessment.

5 LOGISTICS

5.1 Points of Contact

The MITRE POCs for the SCA are listed in Table 2.

Table 10. MITRE Evaluation Team Points of Contact

Name	Position	Phone Number	Email Address
Jim Bielski	Lead Evaluator	(410) 402-2717	jbielski@mitre.org
Seshaddri Nallabola	Application Evaluator	(703) 983-3586	seshaddri@mitre.org
Mehdi Sayed	Application Evaluator	(410) 303-1273	msayed@mitre.org

Table 11. Blue Canopy / Deloitte Points of Contact

Name	Position	Phone Number	Email Address
John Dyson	Lead Evaluator	(703) 762-8086	jodyson@deloitte.com
Farzan Karimi	Application Evaluator	(570) 885-6325	fkarimi@bluecanopy.com
Adam Kerns	Application Evaluator	(703) 340-9973	akerns@bluecanopy.com
Mark Shrout	Application Evaluator	(443) 466-4753	mshrout@bluecanopy.com
Myers Hawkins	Application Evaluator	(334) 413-6792	mhawkins@bluecanopy.com

During assessments, testing problems may be encountered outside normal working hours and require that staff need to be contacted. The CMS POCs for the SCA are listed in Table 3.

Table 12. CMS Points of Contact

Name	Position	Phone Number	Email Address
Tom Schankweiler	CMS/OIS Facilitator	(410) 786-5956	thomas.schankweiler@cms.hhs.gov
Darrin Lyles	CMS/OIS Facilitator	(410) 786-4744	darrin.lyles@cms.hhs.gov
Kirk Grothe	CMS Maintainer	(301) 492-4377	kirk.grothe@cms.hhs.gov
Jim Kerr	Business Owner	(301)-492-4376	james.kerr@cms.hhs.gov
Mark Oh	GTL	(301) 492-4378	mark.oh@cms.hhs.gov

The CGI Federal POCs for the SCA are listed in Table 4.

Table 13. Vendor Points of Contact

Name	Position	Phone Number	Email Address
Lynn Goodrich	Assessment POC and Lead Security Analyst	301-706-9776	lynn.goodrich@cgifederal.com
Greg Caulfield	Secondary Assessment POC and Security Analyst	908-400-1935	greg.caulfield@cgifederal.com

Name	Position	Phone Number	Email Address
Balaji Ramamoorthy	Lead Security Architect and Primary Technical POC	518-461-9590	balajimanikandan.ramamoorthy@cgifederal.com
Mark Calem	HIX Project Manager	703-227-6921	mark.calem@cgifederal.com
Monica Winthrop	HIX Deputy Project Manager	703-227-6012	monica.winthrop@cgifederal.com
Rich McCoy	Plan Management Release Manager	276-889-8854	richard.mccoy@cgifederal.com
Keith Rubin	HIX Chief Architect	973-885-3876	chirayu.desai@cgifederal.com
Joel Singer	IT Operations and Support Manager	703-272-9522	joel.singer@cgifederal.com
Premraj Jeyaprakash	Configuration Manager and System Administrator	703 389 6782	premraj.jeyaprakash@cgifederal.com
Sandeep Johar	Plan Management Technical Lead	571-429-3371	sandeep.johar@cgifederal.com
Pam Rubin	Plan Management Business Requirements Lead	571-533-8605	pamela.rubin@cgifederal.com
Kolap Vanny	Financial Management Release Manager	703-272-6139	kolap.vanny@cgifederal.com
Meg Gill	Financial Management Functional Lead	571-359-7639	marjorie.f.gill@cgifederal.com
Justin Alford	Eligibility & Enrollment Release Manager	571-423-7239	j.alford@cgifederal.com
Vinodh Raman	Individual Appliaction POD Lead	571-535-1691	vinodh.raman@cgifederal.com
Ahmad Ramadani	Plan Compare POD Lead	952-393-9068	ahmad.ramadani@cgifederal.com
Steve Wass	My Account POD Lead	301-412-2288	stephen.wass@cgifederal.com
Prabhakar Thopa	Direct Enrollment POD Lead	571-437-9459	prabhakar.thopa@cgifederal.com
Artan Celepia	Plan Management POD Lead	703-966-6255	artan.celepia@cgifederal.com
Rajeev Sood	Financial Management POD Lead	650-201-6318	rajeev.sood@cgifederal.com
Jim Hewitt	HCP BU ISSO and HCSP Director	617-501-7908	james.hewitt@cgifederal.com

5.2 Technical Staff Requirements

CMS and CGI Federal will need to be available to improve the assessment's efficiency and accuracy. The interactions with MITRE may include technical consultation, supervised access to systems, , facilities, and monitoring assessment activities. Staff may be called upon on in ad-hoc manner via phone, email or in person conversations.

5.3 Onsite Schedule

The anticipated onsite schedule is for a **Kick-off meeting** to be held the morning of Monday September 16, 2013, and more detailed **walkthrough may follow**. Module testing will commence, with the scheduled completion on Friday September 20, 2013. No application interviews will be formally scheduled here. Ad-Hoc application interviews may be performed as needed and agreed upon by MITRE, Blue Canopy and CGI Federal.

Table 14 Onsite Meeting Schedule

Day / Date	Time	Meeting
Mon 9/16	9:30 -10:00	Kick off Meeting
	10:00 - 11:00	Application Walkthroughs
Tue 9/17	4:00 – 4:30	SCA Daily Outbrief
Wed 9/18	4:00 – 4:30	SCA Daily Outbrief
Thu 9/19	4:00 – 4:30	SCA Daily Outbrief
Fri 9/20	4:00 – 4:30	**FINAL** SCA Outbrief

Note that where appropriate, the Business Owner or CMS ISSO is responsible for establishing interview appointments and teleconference bridges. The CMS Facilitator establishes DOB appointments and teleconference bridges.

5.4 Assessment Estimated Timeline

Table 7 describes the estimated timeline for assessment actions and milestones.

Table 15. Estimated Timeline for Assessment Actions and Milestones

Action/Milestone	Description	Date(s)
Perform readiness review	Discuss assessment preparations and ensure tasks (e.g., account creation and providing documentation to MITRE) are on target for completion	Thursday September 12,2013
Establish and test accounts	Set up and test all test accounts for the assessment	Monday September 16, 2013
Finalize and deliver Final Test Plan	Update the final test plan to include all action items, decisions, interview schedules, and other information from the Draft Test Plan Discussion	Tuesday September 17, 2013
Perform onsite assessment	Conduct technical testing and management and operations interviews based on the assessment's scope	September 16-20, 2013
Conduct final out brief	Review and summarize security vulnerabilities	Friday September 20, 2013

Action/Milestone	Description	Date(s)
	from assessment	
Last date to provide remediation evidence (if authorized by CMS Facilitator)	CMS Division of Information Security & Privacy Management strongly advices that the focus of remediation efforts be on addressing High risk findings, followed by Moderate risk findings. ***No application testing will be performed subsequent to the onsite.***	Friday September 20, 2013
Remove security access	Remove security access established for MITRE test accounts	Friday September 20, 2013
Deliver draft report to CMS	Put security vulnerabilities identified during the assessment into report format	Monday September 23, 2013
Review draft report	Answer questions and provide clarification. Only security vulnerabilities reported during the assessment and included in the final out brief are included in the report	Friday September 27, 2013
Deliver final report and data worksheet to CMS	Edit and clarify the draft report and generate a data worksheet	Friday October 4, 2013
Deliver final book package to CMS	Produce and provide hardcopies of test scripts, test data, out briefs, the final report, and the data worksheet(s) with a CD containing this information to the CMS SCAs GTL	Friday October 11, 2013

DEPARTMENT OF HEALTH & HUMAN SERVICES
Centers for Medicare & Medicaid Services
7500 Security Boulevard, Mail Stop N2-14-26
Baltimore, MD 21244-1850

CENTERS FOR MEDICARE & MEDICAID SERVICES

Office of Information Services
7500 Security Boulevard
Baltimore, MD 21244-1850

Health Information eXchange (HIX), Qualified Health Plans (QHP), Dental Module Security Control Assessment (SCA) Report

Final Report

July 15, 2013

CMS SENSITIVE INFORMATION—REQUIRES SPECIAL HANDLING

Table of Contents

List of Tables

List of Figures

1 EXECUTIVE SUMMARY

The Centers for Medicare & Medicaid Services (CMS) of the United States Department of Health and Human Services (HHS) engaged The MITRE Corporation (MITRE) to perform an onsite limited application-only security control assessment (SCA) of the Health Information eXchange (HIX), Qualified Health Plan (QHP)-Dental functionality as part of the CMS Certification and Accreditation (C&A) Program. MITRE conducted an audit to ensure that the functionality complied with CMS security instructions, to determine if security controls were implemented correctly.

1.1 Health Information eXchange (HIX), Qualified Health Plan (QHP) Background

A key provision of the Affordable Care Act (ACA) is the implementation of Insurance Marketplaces (Marketplaces). The Center for Consumer Information and Insurance Oversight (CCIIO) is responsible for providing guidance and oversight for the Marketplaces. A Marketplace is organized to help consumers and small businesses buy health insurance in a way that permits easy comparison of available plan options based on price, benefits and services, and quality. The ACA provides each State with the following options:

- Set up a State-Based Marketplace
- Designate a non-profit entity to operate a State-Based Marketplace
- Collaborate with another state or a consortium to operate a Marketplace
- Defer to the Federally Facilitated Marketplace

The Marketplaces will carry out a number of functions required by the ACA, including certifying Qualified Health Plans (QHP), administering Advance Premium Tax Credits (APTC) and Cost Sharing Reductions (CSR), and providing an easy-to-use website so that individuals can determine eligibility and enroll in health coverage. The Marketplaces will therefore be required to interact with a variety of stakeholders, including consumers, navigators, agents, brokers, employers, Health Plan Issuers, State-based Medicaid and Children's Health Insurance Programs (CHIPs), Federal agencies for verification checks, third-party data sources, and State Insurance Departments. CCIIO intends to guide the States in implementing the Marketplaces by:

- Defining and designing business process models and technical reference models
- Defining and establishing standards and governance structure
- Promoting collaboration, sharing, and reuse
- Using the Application Lifecycle Management (ALM) methodology and a Health and Human Services (HHS) Enterprise Performance Lifecycle (EPLC) model

The CCIIO will manage the Marketplace program and enable collaboration through 1) the use of a cloud-based infrastructure that is Federal Information Security Management Act (FISMA) compliant and can be dynamically scaled as needed, and 2) a secured cloud-based ALM that functions as a component of a Platform as a Service (PaaS). These tools are essential in supporting the following capabilities:

- Management of the numerous stakeholders that are geographically dispersed
- Promotion of modular and service-oriented design
- Reuse and elimination of duplication and redundancy
- Deployment and exercise of practical, Agile project management methodology to oversee a complex national program
- Delivery of a Health Insurance Plan structure for the States, as many have requested such capabilities

1.1.1 Qualified Health Plans

The Plan Management (PM) Qualified Health Plan (QHP) Issuer Certification module of the Federally Facilitated Marketplace (FFM) is a means for the Issuers, States, and the Centers for Medicare and Medicaid Services (CMS) to enter data that can later be used for displaying the plans and benefits for consumers.

Plan Management

The PM business area consists of business processes for acquiring, certifying, monitoring, renewing, and managing the withdrawal of qualified health plans (QHPs) and the Issuers that offer these plans for a given Marketplace. These areas are currently supported by a composite solution consisting of:

- Data submission templates (MS Excel-based) allowing States and Issuers or their representatives to download, populate, validate, and upload into the PM system various complex data sets detailing application, plan, and rate and benefits information.
- User interfaces and services for State and Issuer users to submit, review, modify, and attest to the information uploaded or provided directly via the user interface to support the application and rate and benefits collection process for a given Exchange or set of Exchanges.
- User interfaces and services for CMS personnel to review, monitor, and certify/decertify applications and plans submitted for approval in a given Exchange.
- System interfaces to existing CMS systems (e.g., HIOS) to support streamlined data and profile collection and authentication.

The PM application design is supported by a scalable, 3-tiered environment running on the CMS (b)(5), (b)(6), (b)(7)c, (b)(7)e database. The user interface design is based on the CMS.gov web brand including Healthcare.gov, CMS.gov, and Medicare.gov. It is Section 508 compliant and uses a Progressive Enhancement approach.

Resubmission/Dental

The Resubmission functionality provides the ability for Issuers to resubmit a module for any of the following reasons:

- To address an application deficiency noted by HHS or the State
- To submit a data correction during the plan preview period
- To submit additional information for certification of stand-alone dental plans.

By initiating resubmission, the Issuer is temporarily invalidating the previously submitted QHP application so that information related to one of the aforementioned factors above can be modified and resubmitted. Only applications with a "Cross Validation Completed" status may be resubmitted. Initiating resubmission for any module will change that module status to "Pending Submission" and all other modules to "Validation Completed".

Figure 1 depicts HIX Business Services.

(b)(5), (b)(6), (b)(7)c, (b)(7)e

[redacted]

Table 1 summarizes the core HIX capabilities in each of the business process areas when fully implemented.

Table 1: Core HIX Capabilities

Business Process Area and Purpose	Functional Capabilities	Stakeholders*
Eligibility – Verify and determine consumer's eligibility to obtain insurance through the Marketplace; must also determine potential eligibility for state programs like Medicaid and CHIP.	• Determine eligibility in Medicaid, CHIP, or QHPs based on Modified Adjusted Gross Income (MAGI) and other factors like disability. • Determine eligibility and calculate APTC and CSR; determine eligibility for individual responsibility exemption. • Process eligibility application, interface with the Hub (formerly the Data Services Hub) for validations where required. • Process changes in eligibility. • Facilitate QHP selection. • Interface with the Hub and States as required. • Process appeals and exemptions.	• Consumers (Individuals, Employers, Navigators, Brokers) • The Hub • State Eligibility Systems • Insurers
Enrollment – Enroll eligible consumers in a QHP of their choice.	• Process enrollment choices. • Notify the Hub so that it can notify other Federal agencies and partners. • Support employer enrollment application, enrollment, disenrollment, renewals, and Small Business Health Options Program (SHOP) appeals.	• Consumers (Individuals, Employers, Navigators, Brokers) • The Hub • State Medicaid Enrollment Systems
Plan Management – Procure, certify, and manage Issuers that offer QHPs in the State.	• Capture and display insurer plan data for selection. • Support plan certification, recertification, and decertification processes. • Monitor plan agreements. • Maintain operational plan data to facilitate and create transparency in consumer plan selection. • Provide data for rate review justification.	• Issuers • CMS • State Departments of Insurance

Business Process Area and Purpose	Functional Capabilities	Stakeholders*
Financial Management Services – Perform financial transaction with Issuers and provide support for risk mitigation programs (the three Rs – Reinsurance, Risk Corridors, and Risk Adjustments).	• Collect financial Issuer data. • Perform SHOP and individual premium processing. • Support reconciliation. • Collect data to support risk adjustment program. • Calculate Issuers' credits for risk-mitigation programs (reinsurance, risk corridors, and risk adjustments).	• Insurers • Consumers • State Insurance Actuaries
Quality	• Establish quality benchmarks and metrics for QHPs. • Collect and disseminate data from Issuers, States, and other partners to calculate and disseminate quality metrics.	• Insurers • State Departments of Insurance
Other Federal Functions	• Oversight – Provide mechanisms for Federal government and State HIX authority to oversee, measure, and manage HIX performance. • Others like customer service, communication, etc. are still being defined.	• CMS • State-Based Marketplaces (SBMs)

*Stakeholders/User Roles are inherited from HIOS.

Figure 2 depicts the HIX Concept of Operations (CONOPS) when fully implemented.

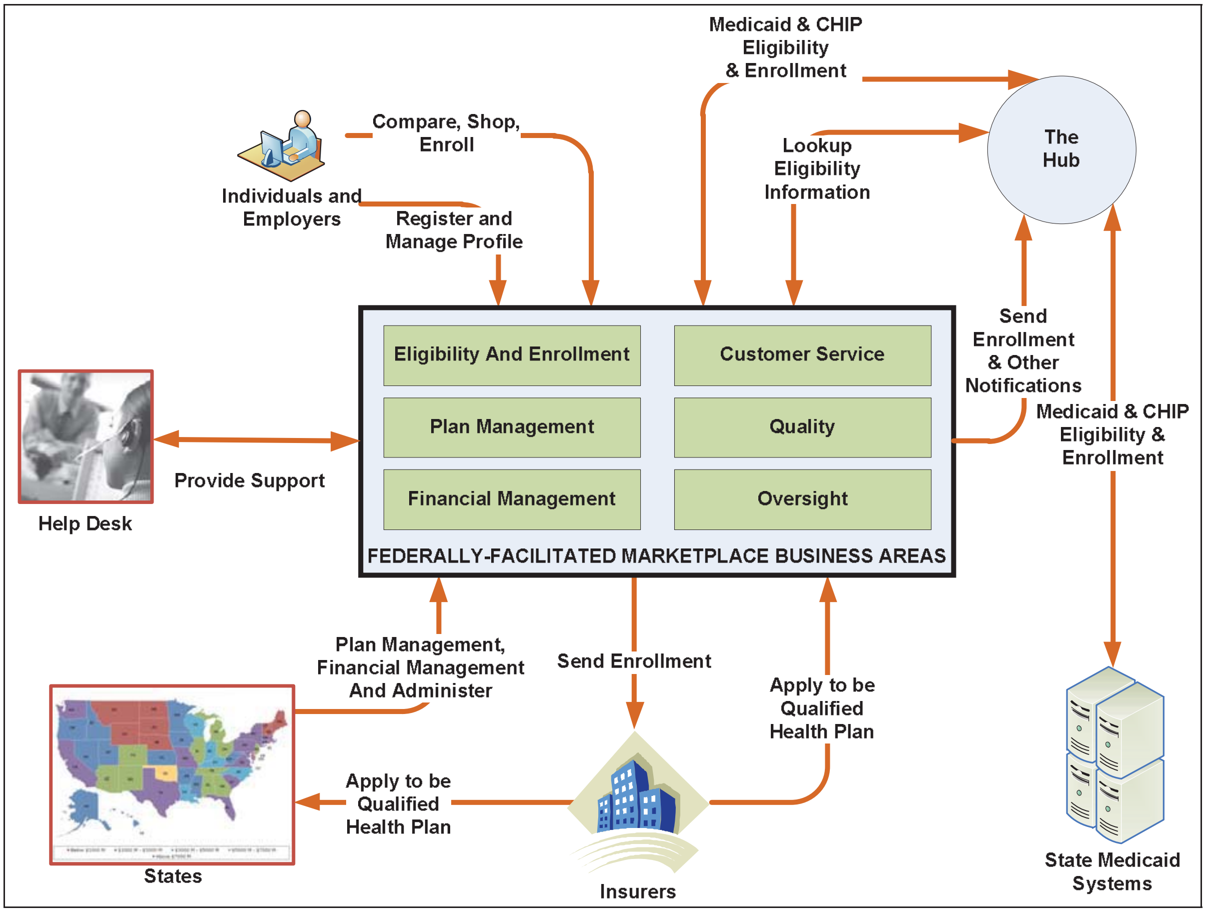
Medicaid & CHIP Eligibility & Enrollment
Compare, Shop, Enroll
The Hub
Lookup Eligibility Information
Individuals and Employers
Register and Manage Profile
Send Enrollment & Other Notifications
Medicaid & CHIP Eligibility & Enrollment
Eligibility And Enrollment
Customer Service
Plan Management
Quality
Financial Management
Oversight
FEDERALLY-FACILITATED MARKETPLACE BUSINESS AREAS
Provide Support
Help Desk
Plan Management, Financial Management And Administer
Send Enrollment
Apply to be Qualified Health Plan
Apply to be Qualified Health Plan
States
Insurers
State Medicaid Systems

Figure 2: HIXHIX Concept of Operations

1.1.2 User Management

All HIX user account lifecycle management is provided by CMS Enterprise Identity Management (EIDM). All HIX user role provisioning and user role management is administered by HIOS Administrators.

HIX has protected content. Access to the protected content requires authentication and authorization through the Remote ID proofing process.

Of the fifteen user types identified for HIX, the following are available to PM users. These users must be authenticated at National Institute of Standards and Technology (NIST) Level 2 prior to accessing HIX. The user types are:

- CMS Staff
- CMS Contractor

- Help Desk
- Administrator
- Reviewer
- Validator
- Attester
- Submitter
- State Reviewer

In future releases, HIX will have both public and protected content. Guest/anonymous users will be permitted to access only public content. Guest access and anonymous access are equivalent; the difference is the Issuers may vary in the terms they use.

When fully implemented, HIX user provisioning and user management will be provided by EIDM (as follows):

- **Create user account:** Users are created when users successfully register with EIDM.
- **Delete user account:** If users' contact information is no longer valid and users' information is no longer referenced in the system, users' accounts are deactivated from EIDM.
- **Update user account:** If users' contact information is no longer valid, users can update their account information in the system.
- **Unlock user account:** If users' accesses are locked during the first time registration with three failed attempts, users' accounts can be unlocked by following instructions provided by EIDM.
- **Deactivate user account:** If users' contact information is no longer valid and is updated with new information, existing relationships are deleted then deactivated, as applicable.
- **Reset password:** If users forget the password but remember the security question/password that was set during their initial registration, users can use the 'Forgot Password' link via the CMS Enterprise Portal (Portal) to reset their passwords. The new password can be used to log into the system. If users forget the security questions/answers and contact the CMS Help Desk for support, the password is reset and an email is sent to users with the reset link to reset the password.

1.1.3 HIX User Access

Enterprise security provides a comprehensive security framework for all HIX components, including physical security controls such as firewalls, Intrusion Detection Systems (IDS), and (b)(5), (b)(6), (b)(7)c, (b)(7)e. It also encompasses the operations, monitoring, and management of all application level security components, such as identity management, authentication, authorization, data security, and Web services security. The computer and infrastructure related security controls are (b)(5), (b)(6), (b)(7)c, (b)(7)e The identity and access control related security controls such as identity management, authentication, and authorization are provided by CMS EIDM. The authorized CMS personnel monitor enterprise security during operations.

The HIX PM module is accessed by Issuers. These users have to access HIX through the Portal. To access the Portal, users have to go through EIDM registration process. The EIDM registration process includes:

- Remote identity proofing (RIDP)
- EIDM account creation
- Issuer user verification

EIDM manages account creation and their life cycle. HIOS manages users' roles and organizational associations (IssuerIDs).

Accounts are created one of two different ways in EIDM:

1. Existing HIOS users who need HIX PM access: These users are extracted from HIOS and are bulk uploaded to EIDM as NIST Level 1 accounts. An email is sent to each uploaded user who has a link to the Portal with a temporary EIDM password. Users access the Portal using the temporary password. Users are required to go through the RIDP process to create a NIST Level 2 account and enter a new password. Upon completion, users can access HIOS or HIX PM as their roles are already established.
2. Users who do not have HIOS access: These users access the Portal, go through the RIDP process, and create an EIDM account. Users then request access to HIOS and/or HIX PM. EIDM requests users' IssuerIDs to confirm if users are Issuers. If users do not know the IssuerID, users are presented with a form to fill out requesting access. The completed form is routed to the HIOS Help Desk. The HIOS Help Desk reviews the request and creates an EIDM account and user roles in HIOS. An email is sent to users with HIOS temporary credentials and an Issuer code. When users access the Portal to request HIOS/HIX PM access, users enter the IssuerID. Upon validation, users are transferred to HIOS. HIOS does not have the EIDM to HIOS account mapping and challenges users for HIOS credentials. Users enter the credentials received in the email and the one time mapping from EIDM to HIOS is completed. Subsequent access to HIX PM and HIOS from the Portal is seamless.

Attachment 2: User Access Flows includes a flow diagram that illustrates the account creation processes described above.

Figure 3 illustrates how an Issuer is authenticated at the Portal using EIDM credentials and subsequently accesses HIX. It also depicts how HIX pulls the roles from HIOS and enforces authorization within HIX using Role Based Access Control (RBAC).

Page 139 redacted for the following reason:
- -
(b)(5), (b)(6), (b)(7)c, (b)(7)e

(b)(5), (b)(6), (b)(7)c, (b)(7)e [redacted]

1.1.4 Data Collection

HIX is a transactional system. All data is collected on the front end through service calls, the Hub, and user interface (UI) modules described below. The data is collected by a diverse user base, including Issuers, consumers, CMS, LMI, National Association of Insurance Commissioners (NAIC), and MIDAS. Data collection begins with templates that ask questions which are presented in the UI in three different applications: the Issuer Application, the Benefit Collection Application, and the Rate Data Collection Application. Data is then collected by one of the UI applications sending calls through the Hub to the PM-API for validation. The data then arrives at the United States Pharmacopeia (USP) Category Class tool in Comma Separated Value (CSV) file format and is processed against some proprietary information. Then the data is sent to the Rate Review Application to collect insurance rate changes. All data collected is stored in the (b)(5), (b)(6), (b)(7)c, (b)(7)e [redacted] system. At this point, there is little to no captured data reporting.

1.1.5 HIX PM-API CMS Issuer Gateway

The intended clients for the CMS Issuer Gateway services are CMS partners in the PM business domain. Typically, these would be HIX systems established by States or systems such as the System for Electronic Rate and Form Filing (SERFF) (deployed by NAIC) that provide PM interfaces to States.

To support their PM business domain, consumers require the following services:

1. Plan information acceptance and validation submitted by Issuers that provide adequate guidance on necessary updates.
2. Validated plan information submission to CMS for attestations from attesting agencies.
3. Utility and ancillary services that help support the overall process of managing the interactions.

The plan information is sent to CMS Issuer Gateway services for validation and submission. The utility services response is in (b)(5), (b)(6), (b)(7)c, (b)(7)e can potentially be large in size since they represent healthcare plans in their entirety or by parts. Some validation and submission inputs are in the form of information batches.

All HIX services or application programming interfaces (APIs) are hosted by the Hub. The Hub is the central conduit for all information exchange related to the Patient Protection and Affordable Care Act (PPACA) with external partners, States and other Federal agencies. CMS partners invoke the services hosted via the Hub. The Hub then interacts with HIX to fulfill the business transaction. For this integration, CMS partners use the Hub's service interface details documented as Business Services Definitions (BSDs).

The Validate and Transform service is the main service exposed by the PM-API. This service (b)(5), (b)(6), (b)(7)c, (b)(7)e represent logical data fragments collected from PM Issuers. It validates the fragment using defined validation rules. If the data is valid, it transforms the input (b)(5), (b)(6), (b)(7)c, (b)(7)e and returns a response. If the validation fails, the service returns an error message. HIX and the Hub have decided to create a polymorphic service interface where all validation requests with Message Transmission Optimization Mechanism(b)(5), (b)(6), (b)(7)c, (b)(7)e (b)(5), (b)(6), (b)(7)c, (b)(7)e and associated metadata are accepted (b)(5), (b)(6), (b)(7)c, (b)(7)e Web service endpoint. This CMS Issuer Gateway service is referred to as "ValidateAndTransformData".

The ValidateAndTransformData service is deployed at the CMS Issuer Gateway. The CMS Issuer Gateway:

1. Receives the transaction (which includes metadata and file attachments) and processes it.
2. Validates the transaction using metadata to confirm that the appropriate transaction files are available for processing.
3. Delegates the file processing responsibility to downstream PM-API services.
4. Relays a response to the Hub to send a notification to the CMS partners when processing completes.

Note: Traditionally CMS has chosen the CMS Enterprise File Transfer (EFT) infrastructure based on the(b)(5), (b)(6), (b)(7)c, (b)(7)e platform to transfer large files. However, for the HIX QHP release, CMS has decided to use Web service-based file transfer services. In addition, CMS assumes the risks associated with transmitting large files over Web services as attachments.

NAIC requires for SERFF consumed services that all validation services must respond with the original (b)(5), (b)(6), (b)(7)c, (b)(7)e to a Microsoft Excel file. This is based on a PM template that the Issuers use to collect data. CMS has approved supporting this requirement with an understanding that this requirement is in addition to PM functionality.

(b)(5), (b)(6), (b)(7)c, (b)(7)e Excel files is processing intensive, and real time responses cannot be guaranteed. Therefore, all SERFF consumed services have deferred Web service responses. In the deferred Web service response paradigm, receiving a request is immediately acknowledged (synchronous response). The processing results are dispatch as a deferred response to be received at a later time. SERFF requires deploying a callback Web service specified by the Hub's BSD to receive a deferred response from the Hub.

1.1.6 Data Transfer Events During a CMS Issuer Gateway Service Invocation

Figure 4 depicts the events in the Hub and HIX at a high-level when processing a CMS Issuer Gateway request.

(b)(5), (b)(6), (b)(7)c, (b)(7)e

HIX CMS Issuer Gateway services are exposed to the SERFF (or similar CMS partner systems) via the Hub. A Hub Proxy service exposes a Web service based on (b)(5), (b)(6), (b)(7)c, (b)(7)e attachments as a proxy to the CMS Issuer Gateway service. This Hub Proxy Web service defines (b)(5), (b)(6), (b)(7)c, (b)(7)e transaction metadata. The service accepts PM (b)(5), (b)(6), (b)(7)c, (b)(7)e (b)(5), (b)(6), (b)(7)c, (b)(7)e

The following sequences depict events that occur during receipt, acknowledgement, processing, and subsequent response of a CMS Issuer Gateway request. Each sequence aggregates a set of events that occur together. Few exception scenarios are highlighted that may occur during a sequence, thereby deviating from the standard processing orchestration.

Sequence 1: SERFF invokes a Hub-hosted CMS Issuer Gateway Web service proxy.

(b)(5), (b)(6), (b)(7)c, (b)(7)e

Exception conditions: In cases where the Hub Proxy Web service is unable to store the attachments or metadata, the service will replace the synchronous acknowledgement with a (b)(5), (b)(6), (b)(7)c, (b)(7)e that the request could not be accepted for processing.

Note: The Hub store-and-forward mechanism for metadata and (b)(5), (b)(6), (b)(7)c, (b)(7)e is confirmed by the Hub team.

Sequence 2: The Hub invokes a CMS Issuer Gateway Web service.

(b)(5), (b)(6), (b)(7)c, (b)(7)e

Exception conditions: In cases where the CMS Issuer Gateway Web service cannot store the attachments or metadata, the service will replace the synchronous acknowledgement with a (b)(5), (b)(6), (b)(7)c, (b)(7)e that the request could not be accepted for processing.

Sequence 3: The CMS Issuer gateway validates transaction metadata.

(b)(5), (b)(6), (b)(7)c, (b)(7)e [redacted]

Exception conditions: If one or more transaction attachment files are unavailable or received files do not match the transaction metadata, the CMS Issuer gateway will send a response to the Hub indicating validation failed. The response includes the appropriate reason and messages. Processing does not continue.

Sequence 4: The CMS Issuer gateway invokes a PM-API batch process.

(b)(5), (b)(6), (b)(7)c, (b)(7)e [redacted]

Sequence 5: The CMS Issuer gateway invokes a Hub callback service to relay transaction response.

(b)(5), (b)(6), (b)(7)c, (b)(7)e [redacted]

Sequence 6: The Hub invokes a SERFF callback service to dispatch transaction response.

(b)(5), (b)(6), (b)(7)c, (b)(7)e [redacted]

(b)(5), (b)(6), (b)(7)c, (b)(7)e

1.2 Assessment Scope

To determine the potential security risks to CMS, MITRE was tasked with providing a limited scope application-only SCA of the Health Information eXchange (HIX), Qualified Health Plan (QHP)-Dental functionality located at the CGI Federal building in Herndon, Va. The Dental functionality was assessed from June 3rd – 7th, 2013. In accordance with the Security Control Assessment Test Plan, MITRE performed the following activities during the independent assessment:

- Performed application security testing
- Reviewed supplied security documentation for the HIX/QHP-Dental functionality

The following CMS Acceptable Risks Safeguards/CMS Minimum Security Requirements (ARS/CMSR) security control families were the focus for the assessment:

- Access Control (AC), all controls except AC-1, AC-18, AC-19, and AC-20
- Awareness and Training (AT), only AT-2 and AT-3
- Audit and Accountability (AU), all controls except AU-1
- Security Assessment and Authorization (CA), all controls except CA-1
- Configuration Management (CM), all controls except CM-1
- Contingency Planning (CP), all controls except CP-1, CP-6, CP-7, CP-8, and CP-9
- Identification and Authentication (IA), all controls except IA-1 and IA-3
- Maintenance (MA), only MA-3
- Media Protection (MP), only MP-5 and MP-6
- Physical and Environmental Protection (PE), only PE-2, PE-5, and PE-17
- Planning (PL), all controls except PL-1 and PL-4
- Personnel Security (PS), all controls except PS-1, PS-2, PS-3, and PS-8
- Risk Assessment (RA), only RA-2 and RA-3
- System and Services Acquisition (SA), all controls except SA-1, SA-7, and SA-9
- System Communications (SC), all controls except SC-1, SC-4, SC-12, SC-17, SC-20, SC-21, SC-22, and SC-32
- System and Information Integrity (SI), all controls except SI-1, SI-3, SI-5, and SI-8

1.3 Summary of Assessment Findings

There were no findings discovered that were specific to the Dental Functionality. The previously report findings for HIX/QHP were validated as still open. No findings spreadsheets were produced.

2 INTRODUCTION

A key provision of the Affordable Care Act (ACA) is the implementation of Insurance Marketplaces (Marketplaces). The Center for Consumer Information and Insurance Oversight (CCIIO) is responsible for providing guidance and oversight for the Marketplaces. A Marketplace is organized to help consumers and small businesses buy health insurance in a way that permits easy comparison of available plan options based on price, benefits and services, and quality. The ACA provides each State with the following options:

- Set up a State-Based Marketplace
- Designate a non-profit entity to operate a State-Based Marketplace
- Collaborate with another state or a consortium to operate a Marketplace
- Defer to the Federally Facilitated Marketplace

The Marketplaces will carry out a number of functions required by the ACA, including certifying Qualified Health Plans (QHP), administering Advance Premium Tax Credits (APTC) and Cost Sharing Reductions (CSR), and providing an easy-to-use website so that individuals can determine eligibility and enroll in health coverage. The Marketplaces will therefore be required to interact with a variety of stakeholders, including consumers, navigators, agents, brokers, employers, Health Plan Issuers, State-based Medicaid and Children's Health Insurance Programs (CHIPs), Federal agencies for verification checks, third-party data sources, and State Insurance Departments. CCIIO intends to guide the States in implementing the Marketplaces by:

- Defining and designing business process models and technical reference models
- Defining and establishing standards and governance structure
- Promoting collaboration, sharing, and reuse
- Using the Application Lifecycle Management (ALM) methodology and a Health and Human Services (HHS) Enterprise Performance Lifecycle (EPLC) model

The CCIIO will manage the Marketplace program and enable collaboration through 1) the use of a cloud-based infrastructure that is Federal Information Security Management Act (FISMA) compliant and can be dynamically scaled as needed, and 2) a secured cloud-based ALM that functions as a component of a Platform as a Service (PaaS). These tools are essential in supporting the following capabilities:

- Management of the numerous stakeholders that are geographically dispersed
- Promotion of modular and service-oriented design
- Reuse and elimination of duplication and redundancy
- Deployment and exercise of practical, Agile project management methodology to oversee a complex national program

- Delivery of a Health Insurance Plan structure for the States, as many have requested such capabilities

Before the MITRE Assessment Team arrived at the site, CGI Federal personnel provided MITRE with various updated documents for the HIX/QHP system which included the System Security Plan (SSP) and Information Security Risk Assessment (ISRA) documents.

2.1 Assessment Methodology

MITRE conducted its SCA of the Health Information eXchange(HIX), Qualified Health Plan (QHP)-Dental functionality located at the CGI Federal Building in Herndon, Va. performed application tests run in the (b)(5), (b)(6), (b)(7)c, (b)(7)e

The purpose of this assessment was to do the following:

- Ensure that the system was in compliance with the *CMS Information Security (IS) Acceptable Risk Safeguards (ARS), Including CMS Minimum Security Requirements (CMSR), Version 1.5,*[1] *CMS Policy for the Information Security Program,*[2] *and CMS Business Partner Systems Security Manual, Version 11.*[3]
- Determine if the application was securely maintained.

The assessment evaluated the system's vulnerability to insider, intranet, and network-based attacks. MITRE used several well-known application testing and scanning tools, in addition to MITRE-developed tools, to conduct a comprehensive vulnerability assessment and system configuration audit.

[1] https://www.cms.gov/informationsecurity/downloads/ARS_App_B_CMSR_Moderate.pdf (07/31/2012),

[2] http://www.cms.hhs.gov/informationsecurity/downloads/PISP.pdf, Version CMS-CIO-POL-SEC02-04.0

[3] http://www.cms.gov/manuals/downloads/117_systems_security.pdf (Sept 30, 2011).

3 DETAILED FINDINGS

Section 3 provides a descriptive analysis of the vulnerabilities identified through the comprehensive SCA process. Each vulnerability is thoroughly explained, specific risks to the continued operations of CMS information systems are identified, and the impact of each risk is analyzed as a business case. The Business Risks also contain suggested corrective actions for closing or reducing the impact of each vulnerability.

Preceding the detailed Business Risks, the methodologies for performing the comprehensive SCA and reporting test results are presented. These sections explain the comprehensive SCA process and describe how the Business Risk Level, Ease-of-Fix, and Estimated Work Effort metrics have been assessed.

3.1 Methodology for Limited Scope Application-Only Security Control Assessment

The overall comprehensive methodology for this assessment provided MITRE with an accurate understanding of the HIX/QHP-Dental functionality to determine if it was configured according to CMS standards. The main objectives of the limited scope application-only SCA were to identify the vulnerabilities and their potential impact.

3.1.1 Limited Scope Application-Only Vulnerability Assessment

The limited scope application-only vulnerability assessment evaluated the system’s vulnerability to insider, and intranet based attacks. To accomplish this objective, MITRE developed an understanding of how the system was configured to determine what an adversary could learn about, and subsequently exploit, in the operational environment.

The limited scope application-only SCA was conducted with full knowledge of the system, products, configurations, and topology. To determine the system configuration and complete a vulnerability assessment of the FFE/QHP-Dental Functionality, MITRE’s SCA looked for the following:

- Improper, weak, or vulnerable configurations
- Non-standard configurations
- Published or known weaknesses, bugs, advisories, and security alerts about specific hardware, software, and networking products used in the system
- Common or known attacks against the specific hardware, software, and networking products used in the system
- Failure to comply with CMS security policies and procedures

3.1.2 Tests and Analyses

The limited scope application-only SCA included a number of tests that methodically analyzed the functionality. The types of tests and analyses MITRE performed during this assessment included the following:

- **Application Assessment—**subjected the application to manual and automated testing to ensure the CIA of data processed by the application
- **Best Engineering Judgment and Various Ad Hoc Tests**—verified that specific requirements, previous recommendations, and conditions had been satisfied
- **Personnel Interviews**—interviewed various personnel involved with the development, training and use of the Dental Functionality.

3.1.3 Tools

MITRE worked with CMS and CGI Federal staff to ensure that industry standard best practices are reflected in CMS's system architecture design. The work performed on this task was accomplished on MITRE-furnished auditing equipment. The tools used by MITRE during the assessment are listed below:

- **Burp Suite** (http://portswigger.net/burp/)—integrated platform for performing security testing of Web applications.
- **Mozilla and Firefox Web Browsers** (http://www.mozilla.org)—open-source Web-based browsers used to manually browse and inspect the Web application and associated forms

3.2 Methodology for Security Test Reporting

The format and content of this report has been developed in accordance with the *CMS Reporting Procedure for Information Security (IS) Assessments, Version 5.0*.[4] The CMS Reporting Standard requires that a Risk Level assessment value be assigned to each Business Risk in order to provide a guideline by which to understand the procedural or technical significance of each finding. Further, an Ease-of-Fix and Estimated Work Effort value must be assigned to each Business Risk to demonstrate how simple or difficult it might be to complete the reasonable and appropriate corrective actions required to close or reduce the impact of each vulnerability. Based on an understanding of the vulnerabilities identified, current CMS implementation of the underlying technology, and the assessment guidelines contained with the *CMS Reporting Procedure for Information Security (IS) Assessments* document, MITRE has assigned these values to each Business Risk.

3.2.1 Risk Level Assessment

Each Business Risk has been assigned a Risk Level value of High, Moderate, or Low. The rating is, in actuality, an assessment of the priority with which each Business Risk will be viewed. The definitions in Table 1 apply to risk level assessment values.

[4] http://www.cms.gov/informationsecurity/downloads/Assessment_Rpting_Procedure.pdf (March 19, 2009).

Table 1. Risk Level Definitions

Rating	Definition of Risk Rating
High	Exploitation of the technical or procedural vulnerability will cause substantial harm to CMS business processes. Significant political, financial, and legal damage is likely to result
Moderate	Exploitation of the technical or procedural vulnerability will significantly impact the confidentiality, integrity and/or availability of the system or data. Exploitation of the vulnerability may cause moderate financial loss or public embarrassment to CMS
Low	Exploitation of the technical or procedural vulnerability will cause minimal impact to CMS operations. The confidentiality, integrity and availability of sensitive information are not at risk of compromise. Exploitation of the vulnerability may cause slight financial loss or public embarrassment

3.2.2 Ease-of-Fix Assessment

Each Business Risk has been assigned an Ease-of-Fix value of Easy, Moderately Difficult, Very Difficult, or No Known Fix. The Ease-of-Fix value is an assessment of how difficult or easy it will be to complete reasonable and appropriate corrective actions required to close or reduce the impact of the vulnerability. The definitions in Table 2 apply to the Ease-of-Fix values.

Table 2. Ease-of-Fix Definitions

Rating	Definition of Ease-of-Fix Rating
Easy	The corrective action(s) can be completed quickly with minimal resources and without causing disruption to the system, or data
Moderately Difficult	Remediation efforts will likely cause a noticeable service disruption: • A vendor patch or major configuration change may be required to close the vulnerability • An upgrade to a different version of the software may be required to address the impact severity • The system may require a reconfiguration to mitigate the threat exposure • Corrective action may require construction or significant alterations to the manner in which business is undertaken
Very Difficult	The high risk of substantial service disruption makes it impractical to complete the corrective action for mission critical systems without careful scheduling: • An obscure, hard-to-find vendor patch may be required to close the vulnerability • Significant, time-consuming configuration changes may be required to address the threat exposure or impact severity • Corrective action requires major construction or redesign of an entire business process

Rating	Definition of Ease-of-Fix Rating
No Known Fix	No known solution to the problem currently exists. The risk may require the business owner to: • Discontinue use of the software or protocol • Isolate the information system within the enterprise, thereby eliminating reliance on the system In some cases, the vulnerability is due to a design-level flaw that cannot be resolved through the application of vendor patches or the reconfiguration of the system. If the system is critical and must be used to support on-going business functions, no less than quarterly monitoring shall be conducted by the business owner and reviewed by CMS IS Management to validate that security incidents have not occurred

3.2.3 Estimated Work Effort Assessment

Each Business Risk has been assigned an Estimated Work Effort value of Minimal, Moderate, Substantial, or Unknown. The Estimated Work Effort value is an assessment of the extent of resources required to complete reasonable and appropriate corrective actions. The definitions in Table 3 apply to the Estimated Work Effort values.

Table 3. Estimated Work Effort Definitions

Rating	Definition of Estimated Work Effort Rating
Minimal	A limited investment of time (i.e., roughly three days or less) is required of a single individual to complete the corrective action(s)
Moderate	A moderate time commitment, up to several weeks, is required of multiple personnel to complete all corrective actions
Substantial	A significant time commitment, up to several months, is required of multiple personnel to complete all corrective actions. Substantial work efforts include the redesign and implementation of CMS network architecture and the implementation of new software, with associated documentation, testing, and training, across multiple CMS organizational units
Unknown	The time necessary to reduce or eliminate the vulnerability is currently unknown

3.2.4 CMS FISMA Controls Tracking System Names

To ensure that the final security controls/findings worksheet can be properly loaded into the CMS FISMA Controls Tracking System (CFACTS), the following system name has been used to populate the HIX/QHP in the Final Management Worksheet delivered as an attachment to this report.

Table 4. CFACTS System Names

CFACTS System Names
HIX

3.3 Business Risks

Management, operational, and technical vulnerabilities representing risks to the secure operation of the HIX/QHP are detailed as findings in this section. Business Risks within this section are technical or procedural in nature, and may result directly in unauthorized access.

To support the *CMS Reporting Procedure for Information Security (IS) Assessments,* the vulnerabilities are ordered in a format that will enable CMS to develop an efficient and workable action plan to remediate all risks. The Business Risks are ordered first by Risk Level from High Risk to Low Risk and then by Estimated Work Effort from Substantial to Minimal. This format will help CMS identify critical risks that must be immediately addressed with little time and effort. Each discussion section identifies the servers or whether the Production or Test environment is impacted by the vulnerability. CMS should initially focus on addressing critical risks that impact the Production environment.

3.3.1 Business Risk Summary

There were no new business risks introduced by the addition of the Dental Functionality to the QHP Application.

4 DOCUMENTATION LISTS

The following tables list the documentation that MITRE requested prior to the onsite visit, as well as documentation provided to MITRE during and after the visit. The tables include the document element number, document title or information requested, and comments. Comments may include the name of the individual, organization, or agency that sent or delivered the documents and the date MITRE received the documents.

Table 5. Documentation Requested Prior to Onsite Visit

Document Element #	Document/Information Requested	Comments
D01	Information System Risk Assessment (ISRA)	L.Goodrich/CGI Federal 5/21/2013
D02	System Security Plan (SSP) • SSP Workbook	L.Goodrich/CGI Federal 5/21/2013
D03	Privacy Impact Assessment (PIA)	L.Goodrich/CGI Federal 5/21/2013
D04	Contingency Plan	L.Goodrich/CGI Federal 5/21/2013
D05	Uniformed Resource Locators (URL) to all Web application interfaces within assessment scope, if not documented in the SDD, VDD, or SSP	B. Ramamoorthy/CGI Federal 5/30/2013
D06	System Design Document (SDD)	N/A
D07	Version Description Document (VDD)	N/A
D08	Interconnection agreements, Memorandum of Understanding (MOU) and/or Interconnection Security Agreement (ISA)	L.Goodrich/CGI Federal 5/21/2013
D09	Rules of Behavior (RoB). Include evidence that RoBs have been acknowledged//signed by users	L.Goodrich/CGI Federal 5/21/2013
D10	Contingency Plan Test	L.Goodrich/CGI Federal 5/21/2013
D11	Configuration and change management process. Include examples of change requests (CR) from request to implementation in production	N/A
D12	Baseline security configurations for each platform and the application within scope and baseline network configurations	N/A
D13	Security Awareness and Training (AT) material. Include evidence of staff who have completed training	N/A
D14	Incident Response (IR) procedures. Include evidence of simulations or actual execution of IR procedures	N/A
D15	Documentation describing the types of audit logging enabled and the established rules for log review and reporting	N/A
D16	Open Corrective Action Plans (CAP) items	N/A

Document Element #	Document/Information Requested	Comments
	from previous SCAs	
D17	System of Record Notice (SORN)	L.Goodrich/CGI Federal 5/21/2013
D18	Operations & Maintenance (O&M) Manual	N/A
D19	Application or system (depending on assessment's scope) backup and storage requirements and procedures. Include data retention and media handling/sanitization procedures	N/A
D20	Detailed system/network architecture diagrams with IP addresses of devices that will be within scope of assessment, if not documented in the SDD, VDD, or SSP)	N/A
D21	Security processes. Include application account creation and account review policy, password policy and malicious, mobile code, and antivirus policy. For password management, ensure policies cover both end user access as well as user accounts used for production operations	N/A
D22	CMS Security Certification Form (if system previously authorized—TAB A)	N/A
D23	Technical Review Board (TRB) and TRA letters. Primarily for major updates and new applications	N/A
D24	Administrator/Operator and User manuals or training materials, if not documented in the SDD, VDD, or SSP)	G Caulfield/CGI Federal 5/31/2013

DEPARTMENT OF HEALTH & HUMAN SERVICES
Centers for Medicare & Medicaid Services
7500 Security Boulevard, Mail Stop N2-14-26
Baltimore, MD 21244-1850

CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES
OFFICE OF INFORMATION SERVICES

CENTERS FOR MEDICARE & MEDICAID SERVICES

Office of Information Services
7500 Security Boulevard
Baltimore, MD 21244-1850

Federal Data Services Hub (DSH) Security Control Assessment (SCA) Report

Final Report

October 4, 2013

CMS SENSITIVE INFORMATION—REQUIRES SPECIAL HANDLING

Table of Contents

List of Tables

List of Figures

1 EXECUTIVE SUMMARY

The Centers for Medicare & Medicaid Services (CMS) of the United States Department of Health and Human Services (HHS) engaged The MITRE Corporation (MITRE) to perform an onsite comprehensive scope security control assessment (SCA) of the Federal Data Services Hub (DSH) major application (MA) as part of the CMS Certification and Accreditation (C&A) Program. MITRE conducted (1) an audit to ensure that the application complied with CMS security instructions, (2) a configuration audit to determine if security controls were implemented correctly, (3) a technical infrastructure test, (4) interviews, and (5) documentation reviews to determine if security controls were implemented correctly.

1.1 FEDERAL DATA SERVICES HUB BACKGROUND

1.1.1 Overview of the Marketplace

The Affordable Care Act directs states to establish State-based Marketplaces by January 1, 2014. In states electing not to establish and operate such a Marketplace, the Affordable Care Act requires the Federal government to establish and operate a Marketplace in the state, referred to as a Federally facilitated Marketplace. The Marketplaces will provide consumers access to health care coverage through private, qualified health plans, and consumers seeking financial assistance may qualify for insurance affordability programs made available through the Marketplace.

The insurance affordability programs include the advance payment of the premium tax credits, cost-sharing reductions, Medicaid, and the Children's Health Insurance Program (CHIP). The advance payment of the premium tax credit may be applied automatically to the purchase of a qualified health plan through the Marketplace, reducing upfront the premiums paid by consumers. Cost-sharing reductions may also lower the amount a consumer has to pay out-of-pocket for deductibles, coinsurance, and copayments for a qualified health plan purchased through the Marketplace. In order to enroll in an insurance affordability program offered through a Marketplace, individuals must complete an application1 and meet certain eligibility requirements. Before we get further into this discussion, it is important to note that while the Marketplace application asks for personal information such as date of birth, name, or address, the Marketplace application never asks for personal health information and the Marketplace IT systems will never access or store personal health information beyond what is normally asked for in Medicaid eligibility applications.

1.1.2 Federal Data Services Hub

CMS has developed a tool, known as the Federal data services hub (the Hub), that provides an electronic connection between the eligibility systems of the Marketplaces to already existing, secure Federal and state databases to verify the information a consumer provides in their Marketplace application. Data transmitted through the Hub will help state agencies determine applicants' eligibility to enroll in Medicaid or CHIP, and help the Federally facilitated and State-based Marketplace eligibility systems determine an applicant's eligibility to seek health insurance coverage through a Marketplace, and their eligibility for advance premium tax credits and cost-sharing reductions.

It is important to understand that the Hub is not a database; it does not retain or store information. It is a routing tool that can validate applicant information from various trusted government databases through secure networks. It allows the Marketplace, Medicaid, and CHIP systems to query the government databases used today in the eligibility processes for many state and Federal programs. The Hub would query only the databases necessary to determine eligibility for specific applicants. The Hub increases efficiency and security by eliminating the need for each Marketplace, Medicaid agency, and CHIP agency to set up separate data connections to each database.

CMS has already completed development and the majority of the testing of the Hub services required to support open enrollment on October 1, 2013. CMS and the Internal Revenue Service (IRS) are currently testing the integration of the Hub with their IT systems, and this testing was 95 percent complete as of the end of June. CMS started testing the Hub with the other Federal partners, including the Social Security Administration (SSA) and the Department of Homeland Security (DHS), earlier this summer, and that testing will be completed by the end of August. CMS is currently testing the Hub with 40 states, and during the remainder of July and August, we will finish testing the Hub with the remaining states and territories.

1.1.3 Description of the Business Process

CMS's Center for Consumer Information and Insurance Oversight (CCIIO) Private Cloud operated by (b)(5), (b)(6), (b)(7)c, (b)(7)e houses the Federal DSH, or the Hub, to support business functions of the State-Based Exchanges (SBEs), Federally Facilitated Exchanges (FFEs), and Federal agencies. The Hub business functions follow:

- Facilitating the exchange of data between SBEs, FFEs, and Federal agencies
- Enabling verification of coverage eligibility
- Providing an aggregation point for the Internal Revenue Service (IRS) when querying for coverage information
- Providing data for oversight of the Exchanges
- Providing data for paying insurers
- Providing data for use in portals for consumers

As such, the Hub sits between SBEs, FFEs, and Federal agencies from a business process standpoint. The figure below depicts the basic Federal DSH concept.

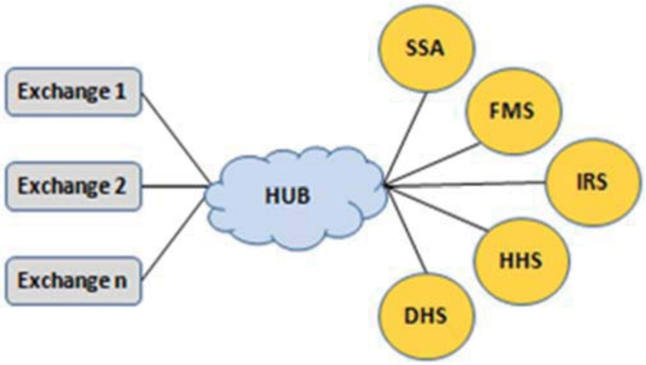

Figure 1: Federal Data Services Hub Concept

To execute these functions, the Hub is dependent on data services provided by SBEs, FFEs, and Federal agencies. Each entity provides Web services available to the Hub for exchanging data, verifying coverage data, and determining eligibility. The Hub uses these Web services to answer requests from entities. The Hub selects the data sources to use when answering a request based on business rules. This may mean that the Hub uses multiple data sources to provide a single answer to a request, which the Hub then returns in a standard format to the requestor. By acting as a central exchange and translation point, the Hub enables the consolidation of security requirements, eliminating the need for each entity to negotiate trusted connections with each other entity. To provide these services to the requestors, the Hub needs to query different data sources for information. Below is listed the business input functions the Hub uses to answer these requests.

Business Input Function	Function Source(s)
Provide individual coverage data	SBE, FFE
Provide income data	IRS, Social Security Administration (SSA)
Provide immigration and citizenship data	Department of Homeland Security (DHS)
Provide incarceration data	DHS
Provide current coverage data	United States Department of Veterans Affairs (VA), TRICARE, Medicaid, Medicare

The Hub provides Web services that requestors may use to take actions or request data from various data sources. Each endpoint acts as a business process. The below table lists the business output functions the Hub provides.

Business Output Function	Supporting Business Process
Processing/Calculation	• Account Transfer • Advance Payment Computation (APC) • Communicate Eligibility

Business Output Function	Supporting Business Process
Verification of eligibility	• Verify Annual Household Income (HHI) and Family Size • Verify Current HHI • Verify Incarceration Status • Verify Lawful Presence (VLP) • Verify Non Employer-Sponsored Insurance (ESI) Minimum Essential Coverage (ESC)

The below table provides a description of each of the supporting business processes.

Business Process Name	Business Process Description
Account Transfer	The Account Transfer Business Service facilitates the transfer of accounts from the requestor to Medicaid/CHIP or from Medicaid/CHIP to the requestor for eligibility determination. This service supports the Exchange-determined Medicaid eligibility based on modified adjusted gross income (MAGI). The Exchange assesses potential Medicaid eligibility based on MAGI and then assesses non-eligibility for Medicaid/CHIP based on MAGI. However, when the individual requests a full Medicaid/CHIP determination, the Exchange assesses potential eligibility for Medicaid based on factors other than MAGI. Additionally, Medicaid/CHIP determines non-eligibility for Medicaid/CHIP. For each of these scenarios, the Exchange or Medicaid/CHIP initiates the same Account Transfer Business Service request to the Hub, which forwards the account to the appropriate agency. The receiving agency performs an eligibility determination for each scenario and returns the eligibility response, if necessary, to the initiator.
Advance Payment Computation	The APC Business Service performs Advance Payment of the Premium Tax Credit (APTC) calculations, determining the maximum amount of monthly APTC for which a household is eligible. The service communicates an applicant's household Income, percentage of Federal Poverty Level (FPL), coverage year, adjusted monthly premium for Second Lowest Cost Silver Plan (SLCSP), and request identifier (ID) to IRS. In the event that the IRS system is down or offline, the Hub performs the APTC calculation for a new application or an update during the benefit year. The Hub maintains the applicable percentage table for each coverage year and updates the table for each year after 2014. CMS staff manually triggers updates. The Hub returns a flag to the requesting party indicating whether IRS or the Hub performed the calculation.
Communicate Eligibility Determination	The Communicate Eligibility Determination Business Service facilitates the storing/writing of an individual's eligibility determination information from various exchanges (FFE & SBEs, Medicaid/CHIP) to the CMS common data store (Federal Exchange Program System (FEPS)). Requestors initiate the same service request to the Hub, which stores/writes the individual's eligibility determination information in the CMS common data store. These requests, with multiple individual records, generally involve the generation and processing of batch (asynchronous) requests by the requestors.

Business Process Name	Business Process Description
Verify Annual Household Income and Family Size	The Verify Annual HHI and Family Size Business Service retrieves tax return information from IRS for use in evaluating taxpayer eligibility and enrollee continued eligibility for insurance affordability programs. The Exchange initiates the service request to the Hub, which forwards the request to IRS. The request communicates applicant full name, Social Security Number (SSN) or Adoption Taxpayer Identification Number (ATIN), and Date of Birth (DOB) to IRS. The Hub adds a name control number before submitting the request to the IRS. IRS provides the Hub with the most recent tax return information on file. For example, an eligibility determination occurs in late 2013 for coverage in 2014, IRS looks first for a 2012 tax return. If no such return is available, IRS may provide information from a 2011 tax return, if a 2011 return is on file. Upon response receipt, the Hub forwards the information back to the requesting party.
Verify Current Household Income	The Verify Current HHI Business Service retrieves the Social Security benefit amount from SSA, quarterly wage information from the trusted data source (TDS), and unemployment insurance income from the TDS. The service uses this information to evaluate applicant eligibility and enrollee continued eligibility for insurance affordability programs by communicating the individual’s full name, SSN, DOB, gender, and State ID to the TDS(s), which provide the Hub with the most recent income information on file at the time of request.
Verify Incarceration Status	The Verify Incarceration Status Business Service assists in determining eligibility by communicating an individual’s full name, DOB, and SSN to SSA to verify applicant incarceration status. The requestor calls the Verify Incarceration Status Business Service when an applicant attests that he/she is not currently incarcerated and inputs an SSN. The Hub then translates the information disclosed by SSA into an incarceration status of Yes, No, or Undisclosed, depending on the combination of information received from SSA by the Hub.
Verify Lawful Presence	The VLP Business Service retrieves immigration status from DHS for use in evaluating eligibility determinations made by the Exchange, and verification of information for participation in Medicaid, the Children’s Health Insurance Program, and the Basic Health Program (BHP). Requestors use this transaction to perform an initial alien status verification using a combination of Alien Number, I-94 Number, Student and Exchange Visitor Information System (SEVIS) ID, Visa Number, Passport Number, Receipt Number, Naturalization Number, and Citizenship Number. DHS processes these requests and responds to the Hub using Agency3InitVerifResp responses. This results in the creation of the DHS case number. The Hub passes this response to the requestor and includes translation for the LawfulPresenceVerified and FiveYearBarIndicator responses. Additionally, the system can use Portable Document Format (PDF) Binary Files with this service to exchange forms from DHS and the requestor. The requestor is also able to make a separate call to close an open case, even if there has not been a resolution.

Business Process Name	Business Process Description
Verify Non-Employer Sponsored Insurance Minimal Essential Coverage	The Verify Non-ESI MEC Business Service determines whether the individual is already eligible for MEC through public health plans, including Medicaid, CHIP, BHP, Medicare, the Veterans Health Program (VHP), TRICARE, and the Peace Corps. Eligibility determination for any one of these programs deems the individual ineligible for the Exchange APTC, and Cost-Sharing Reductions (CSRs). The Exchange accepts the request for verification, triggered by an individual seeking eligibility to enroll in a Qualified Health Plan (QHP), requesting financial assistance, and attesting as not eligible for any of the public health plans: Medicaid, CHIP, BHP, Medicare, TRICARE, VHP, or the Peace Corps. A change in eligibility for other public health plans can also initiate a trigger, if the eligibility determination for any MEC plan changes due to (for example) loss of Medicare coverage. This service then verifies the person is not eligible for that particular plan.

1.2 Assessment Scope

To determine the potential security risks to CMS, MITRE was tasked with providing a comprehensive scope SCA of the DSH MA located at the QSSI facilities located in Columbia, MD. The application was assessed from August 19 – 30, 2013. In accordance with the Security Control Assessment Test Plan, MITRE performed the following activities during the independent assessment:

- Interviewed selected personnel
- Reviewed system baselines
- Reviewed network gear (switch/router/firewall) configurations
- Performed application security testing
- Conducted network vulnerability testing
- Reviewed database configuration settings
- Reviewed supplied security documentation

The following CMS Acceptable Risks Safeguards/CMS Minimum Security Requirements (ARS/CMSR) security control families were the focus for the DSH assessment:

- Access Control (AC)
- Awareness and Training (AT)
- Audit and Accountability (AU)
- Certification, Accreditation and Security Assessments (CA)
- Configuration Management (CM)
- Contingency Planning (CP)
- Identification and Authentication (IA)
- Incident Response (IR)
- Maintenance (MA)
- Media Protection (MP)

- Physical and Environmental Protection (PE)
- Planning (PL)
- Personnel Security (PS)
- Program Management (PM)
- Risk Assessment (RA)
- System and Services Acquisition (SA)
- System and Communications Protection (SC)
- System and Information Integrity (SI)

1.3 Summary of Findings

Of the 38 findings discovered in the system, 4 were considered High risks, 31 Moderate risks, and 3 Low risks. The risks found during the assessment are broken down as shown on the chart in Figure 1.

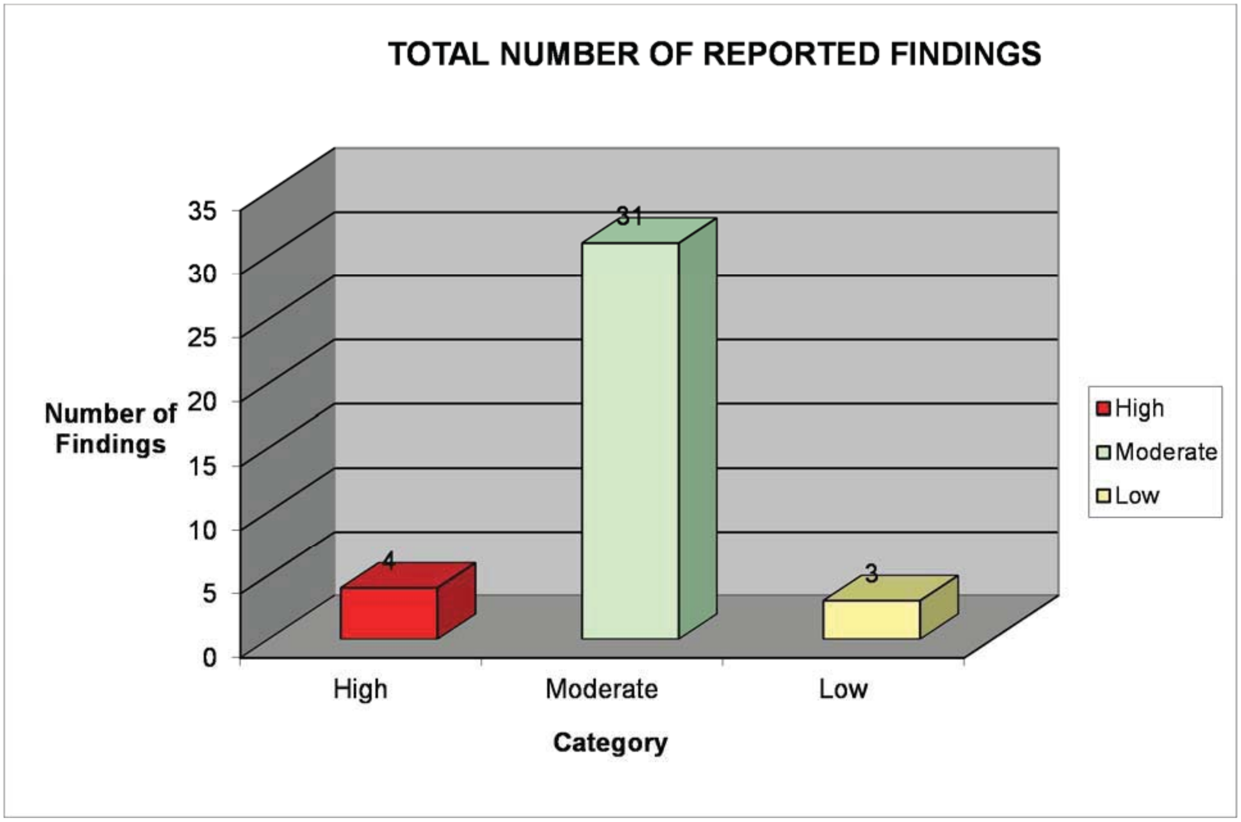

Figure 2~~1~~. Reported Findings by Risk Level

During and after the assessment efforts were made to remediate the findings, with an emphasis on closing High and Moderate risk level findings. Six findings, 4 highs and 2 moderates were remediated. Sixteen findings, 14 Moderates and 2 lows, were already known issues from other systems. One moderate finding was reassigned. As a result, of the 38 initial findings discovered in the system no High risk findings, 14 Moderate risk findings and 1 Low risk finding remain open and assigned to DSH. The risks found during the assessment are broken down as shown on the graph in Figure 2.

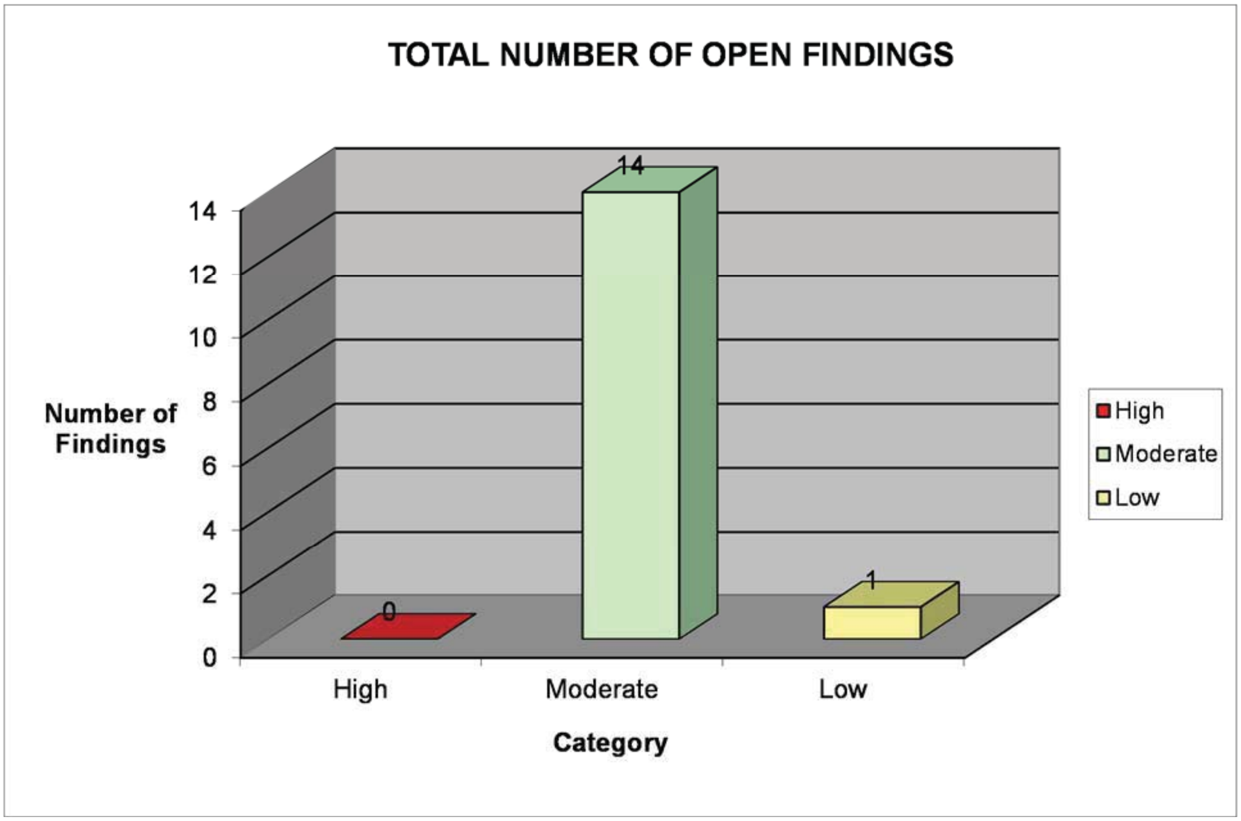

Figure 3~~2~~. Open Findings by Risk Level

The DSH application has a "Moderate" Federal Information Processing Standard (FIPS) impact level since it handles and transports Financial Tax Information (FTI), PII and PHI. 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:

- **Database Management** (b)(5), (b)(6), (b)(7)c, (b)(7)e database configuration settings and password management controls that did not conform to ARS policy which included Password expirations, Account lock times and non-DBA users having access. CMS databases often store valuable routing information. Defense Information Systems Agency (DISA) Secure Technical Implementation Guideline (STIG) and (b)(5), (b)(6), (b)(7)c, (b)(7)e Guide documentation should be consulted to identify security parameters to enable and secure the database**.**
- **Documentation Updates**: Although the CFACTS Workbook, SSP, ISRA, and Contingency Plan conformed to CMS methodologies, suggestions on areas to update with additional information were provided. For example, the system descriptions of databases and the types of data they held did not include all PHI and PII information. Not all known

security risks were conveyed in the ISRA. Detailed analysis of the SSP and ISRA were provided by MITRE. The Privacy Impact Assessment and ISAs were not completed.

1.4 Summary of Recommendations

For each finding, MITRE 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:

- **Strengthen Database Access Controls:** Analyze the security configuration settings of the database servers against industry best practices published by the Defense Information Systems Agency (b)(5), (b)(6), (b)(7)c, (b)(7)e he active accounts as required by the CMS ARS. Document (b)(5), (b)(6), (b)(7)c, (b)(7)e schemes to convey to CMS Business Owners the types of data, PHI/PII, that may reside in the databases, if applicable.
- **Update Documentation:** The System Security Plan (SSP) and Risk Assessment (RA) do not reflect the current technology supporting the environment. Therefore, the documentation does not accurately depict the controls implemented to safeguard the system and data or the risks posed to the environment. Update these documents prior to submitting the Certification and Accreditation package to the Chief Information Security Office (CISO) for the Authorization to Operate (ATO).

2 INTRODUCTION

The Centers for Medicare & Medicaid Services (CMS) of the United States Department of Health and Human Services (HHS) engaged The MITRE Corporation (MITRE) to perform an onsite comprehensive scope security control assessment (SCA) of the Federal Data Services Hub (DSH) major application (MA) as part of the CMS Certification and Accreditation (C&A) Program. MITRE conducted (1) an audit to ensure that the application complied with CMS security instructions, (2) a configuration audit to determine if security controls were implemented correctly, (3) a technical infrastructure test, (4) interviews, and (5) documentation reviews to determine if security controls were implemented correctly.

2.1 FEDERAL DATA SERVICES HUB BACKGROUND

2.1.1 Overview of the Marketplace

The Affordable Care Act directs states to establish State-based Marketplaces by January 1, 2014. In states electing not to establish and operate such a Marketplace, the Affordable Care Act requires the Federal government to establish and operate a Marketplace in the state, referred to as a Federally facilitated Marketplace. The Marketplaces will provide consumers access to health care coverage through private, qualified health plans, and consumers seeking financial assistance may qualify for insurance affordability programs made available through the Marketplace.

The insurance affordability programs include the advance payment of the premium tax credits, cost-sharing reductions, Medicaid, and the Children's Health Insurance Program (CHIP). The advance payment of the premium tax credit may be applied automatically to the purchase of a qualified health plan through the Marketplace, reducing upfront the premiums paid by consumers. Cost-sharing reductions may also lower the amount a consumer has to pay out-of-pocket for deductibles, coinsurance, and copayments for a qualified health plan purchased through the Marketplace. In order to enroll in an insurance affordability program offered through a Marketplace, individuals must complete an application1 and meet certain eligibility requirements.2 Before we get further into this discussion, it is important to note that while the Marketplace application asks for personal information such as date of birth, name, or address, the Marketplace application never asks for personal health information and the Marketplace IT systems will never access or store personal health information beyond what is normally asked for in Medicaid eligibility applications.

2.1.2 Federal Data Services Hub

CMS has developed a tool, known as the Federal data services hub (the Hub), that provides an electronic connection between the eligibility systems of the Marketplaces to already existing, secure Federal and state databases to verify the information a consumer provides in their Marketplace application. Data transmitted through the Hub will help state agencies determine applicants' eligibility to enroll in Medicaid or CHIP, and help the Federally facilitated and State-based Marketplace eligibility systems determine an applicant's eligibility to seek health insurance coverage through a Marketplace, and their eligibility for advance premium tax credits and cost-sharing reductions.

It is important to understand that the Hub is not a database; it does not retain or store information. It is a routing tool that can validate applicant information from various trusted government databases through secure networks. It allows the Marketplace, Medicaid, and CHIP systems to query the government databases used today in the eligibility processes for many state and Federal programs. The Hub would query only the databases necessary to determine eligibility for specific applicants. The Hub increases efficiency and security by eliminating the need for each Marketplace, Medicaid agency, and CHIP agency to set up separate data connections to each database.

CMS has already completed development and the majority of the testing of the Hub services required to support open enrollment on October 1, 2013. CMS and the Internal Revenue Service (IRS) are currently testing the integration of the Hub with their IT systems, and this testing was 95 percent complete as of the end of June. CMS started testing the Hub with the other Federal partners, including the Social Security Administration (SSA) and the Department of Homeland Security (DHS), earlier this summer, and that testing will be completed by the end of August. CMS is currently testing the Hub with 40 states, and during the remainder of July and August, we will finish testing the Hub with the remaining states and territories.

The DSH staff provided MITRE with excellent support during the engagement. Before the MITRE Assessment Team arrived at the site, QSSI personnel provided MITRE with various DSH system-related documents, including the System Security Plan (SSP) and Information Security Risk Assessment (ISRA) documents. Developers, network support, system administrators (SysAdmin), database administrators (DBA), and information security (IS) support personnel were interviewed and questions were answered promptly.

2.2 Assessment Methodology

MITRE conducted its SCA of the DSH MA located at the CMS's Center for Consumer Information and Insurance Oversight (CCIIO) Private Cloud operated (b)(5), (b)(6), (b)(7)c, (b)(7)e (b)(5), (b)(6), (b)(7)c, (b)(7)e The onsite assessment was conducted at the QSSI facilities in Columbia, Maryland. MITRE analyzed the results from network scans, host-based scripts, and application tests run on the DSH environment. MITRE reviewed documentation that was provided and conducted interviews to help determine the overall security posture of the DSH application.

The purpose of this assessment was to do the following:

- Ensure that the system was in compliance with the *CMS Information Security (IS) Acceptable Risk Safeguards (ARS), Including CMS Minimum Security Requirements (CMSR), Version 1.0,*[1] *CMS Technical Reference Architecture, Version 2.0 (TRA),*[2] *CMS*

[1] https://www.cms.gov/informationsecurity/downloads/ARS_App_A_CMSR_HIGH.pdf (07/31/2012), https://www.cms.gov/informationsecurity/downloads/ARS_App_B_CMSR_Moderate.pdf (07/31/2012), https://www.cms.gov/informationsecurity/downloads/ARS_App_C_CMSR_Low.pdf(07/31/2012).

[2] TRA and Supplements can be found on CMS's internal website (November 24, 2009).

Minimum Security Configuration Standards for Operating Systems, Version 4.0,[3] *CMS Policy for the Information Security Program,*[4] *and CMS Business Partner Systems Security Manual, Version 10.6.*[5]

- Determine if the application was securely maintained.
- Ensure that the database was configured properly.

The assessment evaluated the system's vulnerability to insider, intranet, and network-based attacks. It consisted of a technical vulnerability assessment of the underlying infrastructure, a system configuration audit, staff interviews, and documentation reviews. MITRE used several well-known application testing and scanning tools, in addition to MITRE-developed tools, to conduct a comprehensive vulnerability assessment and system configuration audit. MITRE also interviewed staff members tasked with maintaining this system to ensure compliance with the CMS IS ARS/CMSR.

[3] http://www.cms.hhs.gov/cbt/downloads/is_baseline_configs.pdf (February 4, 2010). Only available to authorized users of CMS systems.

[4] http://www.cms.hhs.gov/informationsecurity/downloads/PISP.pdf, Version CMS-CIO-POL-SEC02-03.2 (**Error! Unknown document property name.**).

[5] http://www.cms.gov/manuals/downloads/117_systems_security.pdf (July 17, 2009).

3 DETAILED FINDINGS

Section 3 provides a descriptive analysis of the vulnerabilities identified through the comprehensive SCA process. Each vulnerability is thoroughly explained, specific risks to the continued operations of CMS information systems are identified, and the impact of each risk is analyzed as a business case. The Business Risks also contain suggested corrective actions for closing or reducing the impact of each vulnerability.

Preceding the detailed Business Risks, the methodologies for performing the comprehensive SCA and reporting test results are presented. These sections explain the comprehensive SCA process and describe how the Business Risk Level, Ease-of-Fix, and Estimated Work Effort metrics have been assessed.

3.1 METHODOLOGY FOR COMPREHENSIVE SCOPE SECURITY CONTROL ASSESSMENT

The overall comprehensive methodology for this assessment consisted of a multi-prong approach in which MITRE conducted a technical vulnerability assessment, a system configuration audit, policy compliance audit, and a documentation review. This approach provided MITRE with an accurate understanding of the operational environment of the DSH to determine if it was configured according to CMS standards. The main objectives of the comprehensive scope SCA were to identify the following:

- Vulnerabilities and their potential impact
- Weak system configuration settings that if not changed could compromise the CIA of system data
- Where established CMS security policies have not been followed
- Major discrepancies found in the documentation of the installed systems
- Any weaknesses in the Configuration Management (CM) process

3.1.1 Comprehensive Scope Vulnerability Assessment

The comprehensive scope vulnerability assessment evaluated the system's vulnerability to insider, intranet, and network-based attacks, as well as weaknesses in the management and operational areas of the CCIIO and QSSI Security Programs. To accomplish this objective, MITRE developed an understanding of how the system was configured to determine what an adversary could learn about, and subsequently exploit, in the operational environment.

The comprehensive scope SCA was conducted with full knowledge of the system, products, configurations, and topology. To determine the system configuration and complete a vulnerability assessment of the DSH application, MITRE's SCA looked for the following:

- Improper, weak, or vulnerable configurations
- Non-standard configurations
- Published or known weaknesses, bugs, advisories, and security alerts about specific hardware, software, and networking products used in the system
- Common or known attacks against the specific hardware, software, and networking products used in the system

- Failure to comply with CMS security policies and procedures

3.1.2 Tests and Analyses

The comprehensive scope SCA included a number of tests that methodically analyzed the DSH application and infrastructure. These tests began with high-level scans and then increased in their specificity to include an analysis of each component. The types of tests and analyses MITRE performed during this assessment included the following:

- **Application Assessment—**subjected the thick-client applications to manual and automated testing to ensure the CIA of data processed by the application
- **Automated Scanning**—subjected the infrastructure to the same type of scripted scanning attacks that are available via commercial products and public domain tools
- **Database Scanning—**subjected the underlying database to automated scripts to discover any vulnerabilities in the database configuration
- **System Configuration Assessment**—ran automated scripts and used direct observation to analyze the configuration of network components
- **Best Engineering Judgment and Various Ad Hoc Tests**—verified that specific requirements, previous recommendations, and conditions had been satisfied
- **Personnel Interviews**—interviewed various personnel involved with the daily operational maintenance of the DSH application, as well as other personnel tasked with protecting the system

3.1.3 Tools

MITRE will work with CMS and QSSI staff to ensure that industry standard best practices are reflected in CMS's system architecture design. The work performed on this task was accomplished on MITRE-furnished auditing equipment. The tools used by MITRE during the assessment are listed below:

- **Burp Suite** (http://portswigger.net/burp/)—integrated platform for performing security testing of Web applications.
- **MITRE host-based and database scripts**—scripts developed with the contribution and experience of MITRE's vulnerability and penetration testers. Versions have been developed for both Windows and Unix-based operating systems. With the assistance of SysAdmins, the MITRE Assessment Team uses these scripts to audit operating system security configurations and identify misconfigurations
- **Mozilla and Firefox Web Browsers** (http://www.mozilla.org)—open-source Web-based browsers used to manually browse and inspect the Web application and associated forms
- (b)(5), (b)(6), (b)(7)c, (b)(7)e premier open-source vulnerability assessment tool
- (b)(5), (b)(6), (b)(7)c, (b)(7)e— open source cross-platform solution that provides a graphical interface for rapid creation and execution of soup messages and services.

3.1.4 System Configuration Audit

The main objective of the system configuration audit was to determine if CMS ARS/CMSR security requirements were properly implemented. For this audit, MITRE took the following actions:

- Conducted host-based audits to determine current configurations for each system
- Tested applications and databases for default user accounts
- Tested some of the firewalls, routers, applications, and databases for default user accounts
- Reviewed firewall access control rules
- Reviewed switch configurations
- Determined if system configurations were, or are, in concert with system documentation

3.2 Methodology for Security Test Reporting

The format and content of this report has been developed in accordance with the *CMS Reporting Procedure for Information Security (IS) Assessments, Version 5.0*.[6] The CMS Reporting Standard requires that a Risk Level assessment value be assigned to each Business Risk in order to provide a guideline by which to understand the procedural or technical significance of each finding. Further, an Ease-of-Fix and Estimated Work Effort value must be assigned to each Business Risk to demonstrate how simple or difficult it might be to complete the reasonable and appropriate corrective actions required to close or reduce the impact of each vulnerability. Based on an understanding of the vulnerabilities identified, current CMS implementation of the underlying technology, and the assessment guidelines contained with the *CMS Reporting Procedure for Information Security (IS) Assessments* document, MITRE has assigned these values to each Business Risk.

3.2.1 Risk Level Assessment

Each Business Risk has been assigned a Risk Level value of High, Moderate, or Low. The rating is, in actuality, an assessment of the priority with which each Business Risk will be viewed. The definitions in Table 1~~Table 1~~ apply to risk level assessment values.

Table 1. Risk Level Definitions

Rating	Definition of Risk Rating
High	Exploitation of the technical or procedural vulnerability will cause substantial harm to CMS business processes. Significant political, financial, and legal damage is likely to result
Moderate	Exploitation of the technical or procedural vulnerability will significantly impact the confidentiality, integrity and/or availability of the system or data. Exploitation of the vulnerability may cause moderate financial loss or public embarrassment to CMS
Low	Exploitation of the technical or procedural vulnerability will cause minimal impact to CMS operations. The confidentiality, integrity and availability of sensitive information are not at risk of compromise. Exploitation of the vulnerability may cause slight financial loss or public embarrassment

[6] http://www.cms.gov/informationsecurity/downloads/Assessment_Rpting_Procedure.pdf (March 19, 2009).

Rating	Definition of Risk Rating
Informational	An "Informational" finding, is a risk that has been identified during this assessment which is reassigned to another major application (MA) or General Support System (GSS). The finding must already exist and be open for the reassigned MA or GSS. The informational finding will be noted in a separate section in the final SCA report, but will not be the responsibility of the assessed application to create a Corrective Action Plan, as it is reassigned to the MA or GSS.

3.2.2 Ease-of-Fix Assessment

Each Business Risk has been assigned an Ease-of-Fix value of Easy, Moderately Difficult, Very Difficult, or No Known Fix. The Ease-of-Fix value is an assessment of how difficult or easy it will be to complete reasonable and appropriate corrective actions required to close or reduce the impact of the vulnerability. The definitions in Table 2~~Table 2~~ apply to the Ease-of-Fix values.

Table 2. Ease-of-Fix Definitions

Rating	Definition of Ease-of-Fix Rating
Easy	The corrective action(s) can be completed quickly with minimal resources and without causing disruption to the system, or data
Moderately Difficult	Remediation efforts will likely cause a noticeable service disruption: • A vendor patch or major configuration change may be required to close the vulnerability • An upgrade to a different version of the software may be required to address the impact severity • The system may require a reconfiguration to mitigate the threat exposure • Corrective action may require construction or significant alterations to the manner in which business is undertaken
Very Difficult	The high risk of substantial service disruption makes it impractical to complete the corrective action for mission critical systems without careful scheduling: • An obscure, hard-to-find vendor patch may be required to close the vulnerability • Significant, time-consuming configuration changes may be required to address the threat exposure or impact severity • Corrective action requires major construction or redesign of an entire business process
No Known Fix	No known solution to the problem currently exists. The risk may require the business owner to: • Discontinue use of the software or protocol • Isolate the information system within the enterprise, thereby eliminating reliance on the system In some cases, the vulnerability is due to a design-level flaw that cannot be resolved through the application of vendor patches or the reconfiguration of the system. If the system is critical and must be used to support on-going business functions, no less than quarterly monitoring shall be conducted by the business owner and reviewed by CMS IS Management to validate that security incidents have not occurred

3.2.3 Estimated Work Effort Assessment

Each Business Risk has been assigned an Estimated Work Effort value of Minimal, Moderate, Substantial, or Unknown. The Estimated Work Effort value is an assessment of the extent of resources required to complete reasonable and appropriate corrective actions. The definitions in Table 3~~Table 3~~ apply to the Estimated Work Effort values.

Table 3. Estimated Work Effort Definitions

Rating	Definition of Estimated Work Effort Rating
Minimal	A limited investment of time (i.e., roughly three days or less) is required of a single individual to complete the corrective action(s)
Moderate	A moderate time commitment, up to several weeks, is required of multiple personnel to complete all corrective actions
Substantial	A significant time commitment, up to several months, is required of multiple personnel to complete all corrective actions. Substantial work efforts include the redesign and implementation of CMS network architecture and the implementation of new software, with associated documentation, testing, and training, across multiple CMS organizational units
Unknown	The time necessary to reduce or eliminate the vulnerability is currently unknown

3.2.4 CMS FISMA Controls Tracking System Names

To ensure that the final security controls/findings worksheet can be properly loaded into the CMS FISMA Controls Tracking System (CFACTS), the following system name has been used to populate the System Name field in the Final Management Worksheet delivered as an attachment to this report.

Table 4. CFACTS System Names

CFACTS System Names
DSH

3.3 Business Risks

Management, operational, and technical vulnerabilities representing risks to the secure operation of the DSH are detailed as findings in this section. Business Risks within this section are technical or procedural in nature, and may result directly in unauthorized access.

To support the *CMS Reporting Procedure for Information Security (IS) Assessments,* the vulnerabilities are ordered in a format that will enable CMS to develop an efficient and workable action plan to remediate all risks. The Business Risks are ordered first by Risk Level from High Risk to Low Risk and then by Estimated Work Effort from Substantial to Minimal. This format will help CMS identify critical risks that must be immediately addressed with little time and effort. Each discussion section identifies the servers or whether the Production or Test environment is impacted by the vulnerability. CMS should initially focus on addressing critical risks that impact the Production environment.

3.3.1. BUSINESS RISK	(b)(5)

Applicable Standards:

NIST Security Control Families: Identification and Authentication (IA)

Reference: IA-2

Risk Level: (Risk Level is High, Moderate, or Low)

High

Ease-of-Fix: (Ease-of-Fix is Easy, Moderately Difficult, Very Difficult, or No Known Fix)

Easy

Estimated Work Effort: (Estimated Work Effort is Minimal, Moderate, Substantial, or Unknown; or a time estimate based on level of commitment and an adequate skill set)

Minimal

Description:

3.3.1 DSH 10042013

Finding

(b)(5)

This risk is mapped to row 1 from the initial collection spreadsheet.

(b)(5)

(b)(5)

(b)(5)

Recommended Corrective Action(s):

(b)(5)

3.3.2. BUSINESS RISK

(b)(5) [redacted]

Applicable Standards:

NIST Security Control Families: Configuration Management (CM)

Reference: CM-6

Risk Level: (Risk Level is High, Moderate, or Low)

High

Ease-of-Fix: (Ease-of-Fix is Easy, Moderately Difficult, Very Difficult, or No Known Fix)

Easy

Estimated Work Effort: (Estimated Work Effort is Minimal, Moderate, Substantial, or Unknown; or a time estimate based on level of commitment and an adequate skill set)

Minimal

Description:

3.3.2 DSH 10042013

Finding

(b)(5) [redacted]

This risk is mapped to row 23 from the initial collection spreadsheet.

(b)(5) [redacted]

(b)(5) [redacted]

(b)(5)

Recommended Corrective Action(s):

(b)(5)

3.3.3. BUSINESS RISK

(b)(5)

Applicable Standards:

NIST Security Control Families: Identification and Authentication (IA),
Access Control (AC)

Reference: IA-2, AC-6

Risk Level: (Risk Level is High, Moderate, or Low)

High

Ease-of-Fix: (Ease-of-Fix is Easy, Moderately Difficult, Very Difficult, or No Known Fix)

Easy

Estimated Work Effort: (Estimated Work Effort is Minimal, Moderate, Substantial, or Unknown; or a time estimate based on level of commitment and an adequate skill set)

Minimal

Description:

3.3.3 DSH 10042013

Finding

(b)(5)

This risk is mapped to row 35 from the initial collection spreadsheet.

(b)(5)

(b)(5)

Recommended Corrective Action(s):

(b)(5)

3.3.4. BUSINESS RISK	(b)(5)

Applicable Standards:

NIST Security Control Families: Identification and Authentication (IA)

Reference: IA-2

Risk Level: (Risk Level is High, Moderate, or Low)

High

Ease-of-Fix: (Ease-of-Fix is Easy, Moderately Difficult, Very Difficult, or No Known Fix)

Easy

Estimated Work Effort: (Estimated Work Effort is Minimal, Moderate, Substantial, or Unknown; or a time estimate based on level of commitment and an adequate skill set)

Minimal

Description:

3.3.4 DSH 10042013

Finding

(b)(5)

(b)(5), (b)(6), (b)(7)c, (b)(7)e

This risk is mapped to row 36 from the initial collection spreadsheet.

(b)(5)

(b)(5)

Recommended Corrective Action(s):

(b)(5)

3.3.5. BUSINESS RISK	(b)(5)

Applicable Standards:

NIST Security Control Families: Access Control (AC)

Reference: AC-2

Risk Level: (Risk Level is High, Moderate, or Low)

Moderate

Ease-of-Fix: (Ease-of-Fix is Easy, Moderately Difficult, Very Difficult, or No Known Fix)

Moderately Difficult

Estimated Work Effort: (Estimated Work Effort is Minimal, Moderate, Substantial, or Unknown; or a time estimate based on level of commitment and an adequate skill set)

Substantial

Description:

3.3.5 DSH 10042013

Finding

(b)(5)

This risk is mapped to row 24 from the initial collection spreadsheet.

(b)(5)

(b)(5)

Recommended Corrective Action(s):

(b)(5)

3.3.6. BUSINESS RISK

(b)(5)

Applicable Standards:

NIST Security Control Families: Planning (PL)

Reference: PL-2

Risk Level: (Risk Level is High, Moderate, or Low)

Moderate

Ease-of-Fix: (Ease-of-Fix is Easy, Moderately Difficult, Very Difficult, or No Known Fix)

Easy

Estimated Work Effort: (Estimated Work Effort is Minimal, Moderate, Substantial, or Unknown; or a time estimate based on level of commitment and an adequate skill set)

Moderate

Description:

3.3.6 DSH 10042013

Finding

(b)(5)

This risk is mapped to row 11 from the initial collection spreadsheet.

(b)(5)

(b)(5)

Recommended Corrective Action(s):

(b)(5)

3.3.7. BUSINESS RISK	(b)(5)

Applicable Standards:

NIST Security Control Families: Certification, Accreditation and Security Assessments (CA)

Reference: CA-2

Risk Level: (Risk Level is High, Moderate, or Low)

Moderate

Ease-of-Fix: (Ease-of-Fix is Easy, Moderately Difficult, Very Difficult, or No Known Fix)

Easy

Estimated Work Effort: (Estimated Work Effort is Minimal, Moderate, Substantial, or Unknown; or a time estimate based on level of commitment and an adequate skill set)

Moderate

Description:

3.3.7 DSH 10042013

Finding

(b)(5)

This risk is mapped to row 28 from the initial collection spreadsheet.

(b)(5)

(b)(5)

Recommended Corrective Action(s):

(b)(5)

3.3.8. BUSINESS RISK

(b)(5)

Applicable Standards:

NIST Security Control Families: Systems and Communications Protection (SC)

Reference: SC-7

Risk Level: (Risk Level is High, Moderate, or Low)

Moderate

Ease-of-Fix: (Ease-of-Fix is Easy, Moderately Difficult, Very Difficult, or No Known Fix)

Easy

Estimated Work Effort: (Estimated Work Effort is Minimal, Moderate, Substantial, or Unknown; or a time estimate based on level of commitment and an adequate skill set)

Moderate

Description:

3.3.8 DSH 10042013

Finding

(b)(5)

This risk is mapped to row 37 from the initial collection spreadsheet.

(b)(5)

(b)(5)

Recommended Corrective Action(s):

(b)(5)

3.3.9. BUSINESS RISK	(b)(5) [redacted]

Applicable Standards:

NIST Security Control Families: Systems and Communications Protection (SC)

Reference: SC-2, SC-7

Risk Level: (Risk Level is High, Moderate, or Low)

Moderate

Ease-of-Fix: (Ease-of-Fix is Easy, Moderately Difficult, Very Difficult, or No Known Fix)

Moderately Difficult

Estimated Work Effort: (Estimated Work Effort is Minimal, Moderate, Substantial, or Unknown; or a time estimate based on level of commitment and an adequate skill set)

Moderate

Description:

3.3.9 DSH 10042013

Finding

(b)(5) [redacted]

(b)(5), (b)(6), (b)(7)c, (b)(7)e [redacted]

This risk is mapped to row 38 from the initial collection spreadsheet.

(b)(5) [redacted]

(b)(5)

Recommended Corrective Action(s):

(b)(5)

3.3.10. BUSINESS RISK	(b)(5)

Applicable Standards:

NIST Security Control Families: Contingency Planning (CP)

Reference: CP-2

Risk Level: (Risk Level is High, Moderate, or Low)

Moderate

Ease-of-Fix: (Ease-of-Fix is Easy, Moderately Difficult, Very Difficult, or No Known Fix)

Easy

Estimated Work Effort: (Estimated Work Effort is Minimal, Moderate, Substantial, or Unknown; or a time estimate based on level of commitment and an adequate skill set)

Minimal

Description:

3.3.10 DSH 10042013

Finding

(b)(5)

This risk is mapped to row 10 from the initial collection spreadsheet.

(b)(5)

(b)(5)

Recommended Corrective Action(s):

(b)(5)

3.3.11. BUSINESS RISK	(b)(5)

Applicable Standards:

NIST Security Control Families: Risk Assessment (RA)

Reference: RA-3

Risk Level: (Risk Level is High, Moderate, or Low)

Moderate

Ease-of-Fix: (Ease-of-Fix is Easy, Moderately Difficult, Very Difficult, or No Known Fix)

Easy

Estimated Work Effort: (Estimated Work Effort is Minimal, Moderate, Substantial, or Unknown; or a time estimate based on level of commitment and an adequate skill set)

Minimal

Description:

3.3.11 DSH 10042013

Finding

(b)(5)

This risk is mapped to row 12 from the initial collection spreadsheet.

(b)(5)

(b)(5)

Recommended Corrective Action(s):

(b)(5)

3.3.12. BUSINESS RISK	(b)(5)

Applicable Standards:

NIST Security Control Families: Planning (PL)

Reference: PL-2

Risk Level: (Risk Level is High, Moderate, or Low)

Moderate

Ease-of-Fix: (Ease-of-Fix is Easy, Moderately Difficult, Very Difficult, or No Known Fix)

Easy

Estimated Work Effort: (Estimated Work Effort is Minimal, Moderate, Substantial, or Unknown; or a time estimate based on level of commitment and an adequate skill set)

Minimal

Description:

3.3.12 DSH 10042013

Finding

(b)(5)

This risk is mapped to row 13 from the initial collection spreadsheet.

(b)(5)

(b)(5)

Recommended Corrective Action(s):

(b)(5)

3.3.13. BUSINESS RISK	(b)(5)

Applicable Standards:

NIST Security Control Families: Identification and Authentication (IA)

Reference: IA-5

Risk Level: (Risk Level is High, Moderate, or Low)

Moderate

Ease-of-Fix: (Ease-of-Fix is Easy, Moderately Difficult, Very Difficult, or No Known Fix)

Easy

Estimated Work Effort: (Estimated Work Effort is Minimal, Moderate, Substantial, or Unknown; or a time estimate based on level of commitment and an adequate skill set)

Minimal

Description:

3.3.13 DSH 10042013

Finding

(b)(5)

(b)(5), (b)(6), (b)(7)c, (b)(7)e

This risk is mapped to row 14 from the initial collection spreadsheet.

(b)(5)

(b)(5)

Recommended Corrective Action(s):

(b)(5)

3.3.14. BUSINESS RISK	(b)(5)

Applicable Standards:

NIST Security Control Families: Identification and Authentication (IA)

Reference: IA-5

Risk Level: (Risk Level is High, Moderate, or Low)

Moderate

Ease-of-Fix: (Ease-of-Fix is Easy, Moderately Difficult, Very Difficult, or No Known Fix)

Easy

Estimated Work Effort: (Estimated Work Effort is Minimal, Moderate, Substantial, or Unknown; or a time estimate based on level of commitment and an adequate skill set)

Minimal

Description:

3.3.14 DSH 10042013

Finding

(b)(5)

(b)(5), (b)(6), (b)(7)c, (b)(7)e

This risk is mapped to row 15 from the initial collection spreadsheet.

(b)(5)

(b)(5)

Recommended Corrective Action(s):

(b)(5)

3.3.15. BUSINESS RISK	(b)(5) [redacted]

Applicable Standards:

NIST Security Control Families: Access Control (AC)

Reference: AC-7

Risk Level: (Risk Level is High, Moderate, or Low)

Moderate

Ease-of-Fix: (Ease-of-Fix is Easy, Moderately Difficult, Very Difficult, or No Known Fix)

Easy

Estimated Work Effort: (Estimated Work Effort is Minimal, Moderate, Substantial, or Unknown; or a time estimate based on level of commitment and an adequate skill set)

Minimal

Description:

3.3.15 DSH 10042013

Finding

(b)(5) [redacted]

(b)(5), (b)(6), (b)(7)c, (b)(7)e [redacted]

This risk is mapped to row 16 from the initial collection spreadsheet.

(b)(5) [redacted]

(b)(5) [redacted]

(b)(5)

Recommended Corrective Action(s):

(b)(5)

3.3.16. BUSINESS RISK	(b)(5)

Applicable Standards:

NIST Security Control Families: Access Control (AC)

Reference: AC-6

Risk Level: (Risk Level is High, Moderate, or Low)

Moderate

Ease-of-Fix: (Ease-of-Fix is Easy, Moderately Difficult, Very Difficult, or No Known Fix)

Easy

Estimated Work Effort: (Estimated Work Effort is Minimal, Moderate, Substantial, or Unknown; or a time estimate based on level of commitment and an adequate skill set)

Minimal

Description:

3.3.16 DSH 10042013

Finding

(b)(5)

(b)(5), (b)(6), (b)(7)c, (b)(7)e

This risk is mapped to row 17 from the initial collection spreadsheet.

(b)(5)

(b)(5), (b)(6), (b)(7)c, (b)(7)e

(b)(5), (b)(6), (b)(7)c, (b)(7)e

(b)(5)

Recommended Corrective Action(s):

(b)(5)

3.3.17. BUSINESS RISK	(b)(5)

Applicable Standards:

NIST Security Control Families: Access Control (AC)

Reference: AC-3

Risk Level: (Risk Level is High, Moderate, or Low)

Moderate

Ease-of-Fix: (Ease-of-Fix is Easy, Moderately Difficult, Very Difficult, or No Known Fix)

Easy

Estimated Work Effort: (Estimated Work Effort is Minimal, Moderate, Substantial, or Unknown; or a time estimate based on level of commitment and an adequate skill set)

Minimal

Description:

3.3.17 DSH 10042013

Finding

(b)(5)

(b)(5), (b)(6), (b)(7)c, (b)(7)e

This risk is mapped to row 18 from the initial collection spreadsheet.

(b)(5)

(b)(5)

(b)(5)

Recommended Corrective Action(s):

(b)(5)

3.3.18. BUSINESS RISK	(b)(5) [redacted]

Applicable Standards:

NIST Security Control Families: Audit and Accountability (AU)

Reference: AU-11

Risk Level: (Risk Level is High, Moderate, or Low)

Moderate

Ease-of-Fix: (Ease-of-Fix is Easy, Moderately Difficult, Very Difficult, or No Known Fix)

Easy

Estimated Work Effort: (Estimated Work Effort is Minimal, Moderate, Substantial, or Unknown; or a time estimate based on level of commitment and an adequate skill set)

Minimal

Description:

3.3.18 DSH 10042013

Finding

(b)(5) [redacted]

(b)(5), (b)(6), (b)(7)c, (b)(7)e [redacted]

This risk is mapped to row 19 from the initial collection spreadsheet.

(b)(5) [redacted]

(b)(5) [redacted]

Recommended Corrective Action(s):

(b)(5)

### 3.3.19. BUSINESS RISK	(b)(5)

Applicable Standards:

NIST Security Control Families: Certification, Accreditation and Security Assessments (CA)

Reference: CA-3

Risk Level: (Risk Level is High, Moderate, or Low)

Moderate

Ease-of-Fix: (Ease-of-Fix is Easy, Moderately Difficult, Very Difficult, or No Known Fix)

Easy

Estimated Work Effort: (Estimated Work Effort is Minimal, Moderate, Substantial, or Unknown; or a time estimate based on level of commitment and an adequate skill set)

Minimal

Description:

3.3.19 DSH 10042013

Finding

(b)(5)

This risk is mapped to row 26 from the initial collection spreadsheet.

(b)(5)

(b)(5)

Recommended Corrective Action(s):

(b)(5)

3.3.20. BUSINESS RISK	(b)(5)

Applicable Standards:

NIST Security Control Families: Planning (PL)

Reference: PL-5

Risk Level: (Risk Level is High, Moderate, or Low)

Moderate

Ease-of-Fix: (Ease-of-Fix is Easy, Moderately Difficult, Very Difficult, or No Known Fix)

Easy

Estimated Work Effort: (Estimated Work Effort is Minimal, Moderate, Substantial, or Unknown; or a time estimate based on level of commitment and an adequate skill set)

Minimal

Description:

3.3.20 DSH 10042013

Finding

(b)(5)

This risk is mapped to row 29 from the initial collection spreadsheet.

(b)(5)

Recommended Corrective Action(s):

(b)(5)

3.3.21. BUSINESS RISK	(b)(5)

Applicable Standards:

NIST Security Control Families: Risk Assessment (RA)

Reference: RA-3

Risk Level: (Risk Level is High, Moderate, or Low)

Low

Ease-of-Fix: (Ease-of-Fix is Easy, Moderately Difficult, Very Difficult, or No Known Fix)

Moderately Difficult

Estimated Work Effort: (Estimated Work Effort is Minimal, Moderate, Substantial, or Unknown; or a time estimate based on level of commitment and an adequate skill set)

Moderate

Description:

3.3.21 DSH 10042013

Finding

(b)(5)

This risk is mapped to row 34 from the initial collection spreadsheet.

(b)(5)

(b)(5)

Recommended Corrective Action(s):

(b)(5)

3.4 Informational Risks

(b)(5)

3.4.1 BUSINESS RISK	(b)(5)

Applicable Standards:

NIST Security Control Families: Access Control (AC)

Reference: AC-8

Risk Level: (Risk Level is High, Moderate, or Low)

Low

Ease-of-Fix: (Ease-of-Fix is Easy, Moderately Difficult, Very Difficult, or No Known Fix)

Easy

Estimated Work Effort: (Estimated Work Effort is Minimal, Moderate, Substantial, or Unknown; or a time estimate based on level of commitment and an adequate skill set)

Minimal

Description:

3.4.1 DSH 10042013

Finding

(b)(5)

(b)(5), (b)(6), (b)(7)c, (b)(7)e

This risk is mapped to row 22 from the initial collection spreadsheet.

(b)(5)

(b)(5)

Recommended Corrective Action(s):

(b)(5)

3.4.2 BUSINESS RISK	(b)(5) [redacted]

Applicable Standards:

NIST Security Control Families: Configuration Management (CM)

Reference: CM-6

Risk Level: (Risk Level is High, Moderate, or Low)

Low

Ease-of-Fix: (Ease-of-Fix is Easy, Moderately Difficult, Very Difficult, or No Known Fix)

Easy

Estimated Work Effort: (Estimated Work Effort is Minimal, Moderate, Substantial, or Unknown; or a time estimate based on level of commitment and an adequate skill set)

Minimal

Description:

3.4.2 DSH 10042013

Finding

(b)(5) [redacted]

(b)(5), (b)(6), (b)(7)c, (b)(7)e [redacted]

This risk is mapped to row 25 from the initial collection spreadsheet.

(b)(5) [redacted]

(b)(5)

Recommended Corrective Action(s):

(b)(5)

3.4.3 BUSINESS RISK

(b)(5)

Applicable Standards:

NIST Security Control Families: Contingency Planning (CP)

Reference: CP-7

Risk Level: (Risk Level is High, Moderate, or Low)

Moderate

Ease-of-Fix: (Ease-of-Fix is Easy, Moderately Difficult, Very Difficult, or No Known Fix)

Very Difficult

Estimated Work Effort: (Estimated Work Effort is Minimal, Moderate, Substantial, or Unknown; or a time estimate based on level of commitment and an adequate skill set)

Substantial

Description:

3.4.3 DSH 10042013

Finding

(b)(5)

This risk is mapped to row 27 from the initial collection spreadsheet.

(b)(5)

(b)(5)

Recommended Corrective Action(s):

(b)(5)

3.4.4 BUSINESS RISK	(b)(5)

Applicable Standards:

NIST Security Control Families: Audit and Accountability (AU)

Reference: AU-2, AU-12

Risk Level: (Risk Level is High, Moderate, or Low)

Moderate

Ease-of-Fix: (Ease-of-Fix is Easy, Moderately Difficult, Very Difficult, or No Known Fix)

Moderately Difficult

Estimated Work Effort: (Estimated Work Effort is Minimal, Moderate, Substantial, or Unknown; or a time estimate based on level of commitment and an adequate skill set)

Moderate

Description:

3.4.4 DSH 10042013

Finding

(b)(5)

(b)(5), (b)(6), (b)(7)c, (b)(7)e

This risk is mapped to row 4 from the initial collection spreadsheet.

(b)(5)

(b)(5)

Recommended Corrective Action(s):

(b)(5)

3.4.5 BUSINESS RISK	(b)(5)

Applicable Standards:

NIST Security Control Families: System And Information Integrity (SI)

Reference: SI-2

Risk Level: (Risk Level is High, Moderate, or Low)

Moderate

Ease-of-Fix: (Ease-of-Fix is Easy, Moderately Difficult, Very Difficult, or No Known Fix)

Easy

Estimated Work Effort: (Estimated Work Effort is Minimal, Moderate, Substantial, or Unknown; or a time estimate based on level of commitment and an adequate skill set)

Minimal

Description:

3.4.5 DSH 10042013

Finding

(b)(5)

(b)(5), (b)(6), (b)(7)c, (b)(7)e

This risk is mapped to row 2 from the initial collection spreadsheet.

(b)(5)

1

(b)(5)

Recommended Corrective Action(s):

(b)(5)

3.4.6 BUSINESS RISK

(b)(5) [redacted]

Applicable Standards:

NIST Security Control Families: Access Control (AC)

Reference: AC-3.1

Risk Level: (Risk Level is High, Moderate, or Low)

Moderate

Ease-of-Fix: (Ease-of-Fix is Easy, Moderately Difficult, Very Difficult, or No Known Fix)

Easy

Estimated Work Effort: (Estimated Work Effort is Minimal, Moderate, Substantial, or Unknown; or a time estimate based on level of commitment and an adequate skill set)

Minimal

Description:

3.4.6 DSH 10042013

Finding

(b)(5) [redacted]

(b)(5), (b)(6), (b)(7)c, (b)(7)e [redacted]

This risk is mapped to row 3 from the initial collection spreadsheet.

(b)(5) [redacted]

(b)(5)

Recommended Corrective Action(s):

(b)(5)

3.4.7 BUSINESS RISK

(b)(5), (b)(6), (b)(7)c, (b)(7)e [redacted]

Applicable Standards:

NIST Security Control Families: Audit And Accountability (AU)

Reference: AU-6(1)

Risk Level: (Risk Level is High, Moderate, or Low)

Moderate

Ease-of-Fix: (Ease-of-Fix is Easy, Moderately Difficult, Very Difficult, or No Known Fix)

Easy

Estimated Work Effort: (Estimated Work Effort is Minimal, Moderate, Substantial, or Unknown; or a time estimate based on level of commitment and an adequate skill set)

Minimal

Description:

3.4.7 DSH 10042013

Finding

(b)(5) [redacted]

(b)(5), (b)(6), (b)(7)c, (b)(7)e [redacted]

This risk is mapped to row 5 from the initial collection spreadsheet.

(b)(5)

Recommended Corrective Action(s):

(b)(5)

3.4.8 BUSINESS RISK

(b)(5) [redacted]

Applicable Standards:

NIST Security Control Families: Configuration Management (CM)

Reference: CM-6

Risk Level: (Risk Level is High, Moderate, or Low)

Moderate

Ease-of-Fix: (Ease-of-Fix is Easy, Moderately Difficult, Very Difficult, or No Known Fix)

Easy

Estimated Work Effort: (Estimated Work Effort is Minimal, Moderate, Substantial, or Unknown; or a time estimate based on level of commitment and an adequate skill set)

Minimal

Description:

3.4.8 DSH 10042013

Finding

(b)(5) [redacted]

(b)(5), (b)(6), (b)(7)c, (b)(7)e [redacted]

This risk is mapped to row 6 from the initial collection spreadsheet.

(b)(5) [redacted]

(b)(5)

(b)(5)

Recommended Corrective Action(s):

(b)(5)

3.4.9 BUSINESS RISK	(b)(5)

Applicable Standards:

NIST Security Control Families: Identification and Authentication (IA)

Reference: IA-5

Risk Level: (Risk Level is High, Moderate, or Low)

Moderate

Ease-of-Fix: (Ease-of-Fix is Easy, Moderately Difficult, Very Difficult, or No Known Fix)

Easy

Estimated Work Effort: (Estimated Work Effort is Minimal, Moderate, Substantial, or Unknown; or a time estimate based on level of commitment and an adequate skill set)

Minimal

Description:

3.4.9 DSH 10042013

Finding

(b)(5)

(b)(5), (b)(6), (b)(7)c, (b)(7)e

This risk is mapped to row 7 from the initial collection spreadsheet.

(b)(5)

(b)(5)

(b)(5)

(b)(5), (b)(6), (b)(7)c, (b)(7)e

Recommended Corrective Action(s):

(b)(5)

3.4.10 BUSINESS RISK	(b)(5) [redacted]

Applicable Standards:

NIST Security Control Families: Configuration Management (CM)

Reference: CM-6

Risk Level: (Risk Level is High, Moderate, or Low)

Moderate

Ease-of-Fix: (Ease-of-Fix is Easy, Moderately Difficult, Very Difficult, or No Known Fix)

Easy

Estimated Work Effort: (Estimated Work Effort is Minimal, Moderate, Substantial, or Unknown; or a time estimate based on level of commitment and an adequate skill set)

Minimal

Description:

3.4.10 DSH 10042013

Finding

(b)(5) [redacted]

(b)(5), (b)(6), (b)(7)c, (b)(7)e [redacted]

This risk is mapped to row 8 from the initial collection spreadsheet.

(b)(5)

[redacted]

Recommended Corrective Action(s):

(b)(5)

[redacted]

3.4.11 BUSINESS RISK	(b)(5)

Applicable Standards:

NIST Security Control Families: Access Control (AC)

Reference: AC-3.1

Risk Level: (Risk Level is High, Moderate, or Low)

Moderate

Ease-of-Fix: (Ease-of-Fix is Easy, Moderately Difficult, Very Difficult, or No Known Fix)

Easy

Estimated Work Effort: (Estimated Work Effort is Minimal, Moderate, Substantial, or Unknown; or a time estimate based on level of commitment and an adequate skill set)

Minimal

Description:

3.4.11 DSH 10042013

Finding

(b)(5)

(b)(5), (b)(6), (b)(7)c, (b)(7)e

This risk is mapped to row 9 from the initial collection spreadsheet.

(b)(5)

(b)(5)

Recommended Corrective Action(s):

(b)(5)

3.4.12 BUSINESS RISK

(b)(5)

Applicable Standards:

NIST Security Control Families: System And Information Integrity (SI)

Reference: SI-2

Risk Level: (Risk Level is High, Moderate, or Low)

Moderate

Ease-of-Fix: (Ease-of-Fix is Easy, Moderately Difficult, Very Difficult, or No Known Fix)

Easy

Estimated Work Effort: (Estimated Work Effort is Minimal, Moderate, Substantial, or Unknown; or a time estimate based on level of commitment and an adequate skill set)

Minimal

Description:

3.4.12 DSH 10042013

Finding

(b)(5)

(b)(5), (b)(6), (b)(7)c, (b)(7)e

This risk is mapped to row 20 from the initial collection spreadsheet.

(b)(5)

(b)(5)

Recommended Corrective Action(s):

(b)(5)

3.4.13 BUSINESS RISK	(b)(5) [redacted]

Applicable Standards:

NIST Security Control Families: Identification and Authentication (IA)

Reference: IA-5

Risk Level: (Risk Level is High, Moderate, or Low)

Moderate

Ease-of-Fix: (Ease-of-Fix is Easy, Moderately Difficult, Very Difficult, or No Known Fix)

Easy

Estimated Work Effort: (Estimated Work Effort is Minimal, Moderate, Substantial, or Unknown; or a time estimate based on level of commitment and an adequate skill set)

Minimal

Description:

3.4.13 DSH 10042013

Finding

(b)(5) [redacted]

(b)(5), (b)(6), (b)(7)c, (b)(7)e [redacted]

This risk is mapped to row 21 from the initial collection spreadsheet.

(b)(5)

(b)(5)

(b)(5)

Recommended Corrective Action(s):

(b)(5)

3.4.14 BUSINESS RISK	(b)(5) [redacted]

Applicable Standards:

NIST Security Control Families: Access Control (AC)

Reference: AC-7

Risk Level: (Risk Level is High, Moderate, or Low)

Moderate

Ease-of-Fix: (Ease-of-Fix is Easy, Moderately Difficult, Very Difficult, or No Known Fix)

Easy

Estimated Work Effort: (Estimated Work Effort is Minimal, Moderate, Substantial, or Unknown; or a time estimate based on level of commitment and an adequate skill set)

Minimal

Description:

3.4.14 DSH 10042013

Finding

(b)(5) [redacted]

(b)(5), (b)(6), (b)(7)c, (b)(7)e [redacted]

This risk is mapped to row 30 from the initial collection spreadsheet.

(b)(5) [redacted]

(b)(5)

Recommended Corrective Action(s):

(b)(6)

3.4.15 BUSINESS RISK	(b)(5) [redacted]

Applicable Standards:

NIST Security Control Families: Configuration Management (CM)

Reference: CM-6

Risk Level: (Risk Level is High, Moderate, or Low)

Moderate

Ease-of-Fix: (Ease-of-Fix is Easy, Moderately Difficult, Very Difficult, or No Known Fix)

Easy

Estimated Work Effort: (Estimated Work Effort is Minimal, Moderate, Substantial, or Unknown; or a time estimate based on level of commitment and an adequate skill set)

Minimal

Description:

3.4.15 DSH 10042013

Finding

(b)(5) [redacted]

(b)(5), (b)(6), (b)(7)c, (b)(7)e [redacted]

This risk is mapped to row 31 from the initial collection spreadsheet.

(b)(5) [redacted]

(b)(5)

Recommended Corrective Action(s):

(b)(5)

3.4.16 BUSINESS RISK	(b)(5) [redacted]

Applicable Standards:

NIST Security Control Families: Access Control (AC)

Reference: AC-2(3)

Risk Level: (Risk Level is High, Moderate, or Low)

Moderate

Ease-of-Fix: (Ease-of-Fix is Easy, Moderately Difficult, Very Difficult, or No Known Fix)

Easy

Estimated Work Effort: (Estimated Work Effort is Minimal, Moderate, Substantial, or Unknown; or a time estimate based on level of commitment and an adequate skill set)

Minimal

Description:

3.4.16 DSH 10042013

Finding

(b)(5) [redacted]

(b)(5), (b)(6), (b)(7)c, (b)(7)e [redacted]

This risk is mapped to row 33 from the initial collection spreadsheet.

(b)(5) [redacted]

(b)(5)

Recommended Corrective Action(s):

(b)(5)

3.5 REASSIGNED BUSINESS RISK

(b)(5)

3.5.1 Business Risk	(b)(5)

Applicable Standards:

NIST Security Control Families: Identification and Authentication (IA)

Reference: IA-5(1)

Risk Level: (Risk Level is High, Moderate, or Low)

Moderate

Ease-of-Fix: (Ease-of-Fix is Easy, Moderately Difficult, Very Difficult, or No Known Fix)

Easy

Estimated Work Effort: (Estimated Work Effort is Minimal, Moderate, Substantial, or Unknown; or a time estimate based on level of commitment and an adequate skill set)

Minimal

Description:

3.5.1 DSH 10042013

Finding

(b)(5)

(b)(5), (b)(6), (b)(7)c, (b)(7)e

This risk is mapped to row 32 from the initial collection spreadsheet.

(b)(5)

(b)(5)

Recommended Corrective Action(s):

(b)(5)

4 DOCUMENTATION LISTS

The following tables list the documentation that MITRE requested prior to the onsite visit, as well as documentation provided to MITRE during and after the visit. The tables include the document element number, document title or information requested, and comments. Comments may include the name of the individual, organization, or agency that sent or delivered the documents and the date MITRE received the documents.

Table 5. Documentation Requested Prior to Onsite Visit

Document Element #	Document/Information Requested	Comments
D01	Information System Risk Assessment (ISRA)	
D02	System Security Plan (SSP) • SSP Workbook	
D03	Privacy Impact Assessment (PIA)	
D04	Contingency Plan	
D05	Uniformed Resource Locators (URL) to all Web application interfaces within assessment scope, if not documented in the SDD, VDD, or SSP	
D06	System Design Document (SDD)	
D07	Version Description Document (VDD)	
D08	Interconnection agreements, Memorandum of Understanding (MOU) and/or Interconnection Security Agreement (ISA)	
D09	Rules of Behavior (RoB). Include evidence that RoBs have been acknowledged//signed by users	
D10	Contingency Plan Test	
D11	Configuration and change management process. Include examples of change requests (CR) from request to implementation in production	
D12	Baseline security configurations for each platform and the application within scope and baseline network configurations	
D13	Security Awareness and Training (AT) material. Include evidence of staff who have completed training	
D14	Incident Response (IR) procedures. Include evidence of simulations or actual execution of IR procedures	
D15	Documentation describing the types of audit logging enabled and the established rules for log review and reporting	
D16	Open Corrective Action Plans (CAP) items from previous SCAs	
D17	System of Record Notice (SORN)	

Document Element #	Document/Information Requested	Comments
D18	Operations & Maintenance (O&M) Manual	
D19	Application or system (depending on assessment's scope) backup and storage requirements and procedures. Include data retention and media handling/sanitization procedures	
D20	Detailed system/network architecture diagrams with IP addresses of devices that will be within scope of assessment, if not documented in the SDD, VDD, or SSP)	
D21	Security processes. Include application account creation and account review policy, password policy and malicious, mobile code, and antivirus policy. For password management, ensure policies cover both end user access as well as user accounts used for production operations	
D22	CMS Security Certification Form (if system previously authorized—TAB A)	
D23	Technical Review Board (TRB) and TRA letters. Primarily for major updates and new applications	
D24	Administrator/Operator and User manuals or training materials, if not documented in the SDD, VDD, or SSP)	

CENTERS FOR MEDICARE & MEDICAID SERVICES

OFFICE OF INFORMATION SERVICES
7500 Security Boulevard
Baltimore, MD 21244-1850

Health Information eXchange (HIX), Quality Health Plans (QHP), August 2013 Security Controls Assessment Test Plan

August 21, 2013

FINAL

Table of Contents

List of Tables

1 INTRODUCTION

1.1 Purpose

This document describes the security controls assessment (SCA) methodology, schedule, and requirements that The MITRE Corporation (MITRE) will use to evaluate the Health Information eXchange (HIX) modules that were not tested previsouly. Specifically, the Plan Management(PM), Financial Management(FM) and the Enrollemnt and Eligibility (E&E) modules. The goal of the SCA test plan is to explain clearly the information MITRE expects to obtain prior to the assessment, the areas that will be examined, and the proposed scheduled activities MITRE expects to perform during the assessment. This document is meant to be used by the Centers for Medicare & Medicaid Services (CMS) and CGI Federal technical managers, network engineers, and system administrators responsible for system operations.

1.2 Security Controls Assessment Background

MITRE operates a federally funded research and development center (FFRDC) providing services to the government in accordance with the provisions and limitations defined in the Federal Acquisition Regulation (FAR) part 35.017. According to this regulation, in order for an FFRDC to discharge its responsibilities to the sponsoring agency, it must have access to government and supplier data (e.g., sensitive and proprietary data) and to employees and facilities beyond that which is common to the normal contractual relationship. As an FFRDC agent, MITRE is required to conduct its business in a manner befitting its special relationship with the government, to operate in the public interest with objectivity and independence, to be free from organizational conflicts of interest, and to have full disclosure of its affairs to the sponsoring agency.

MITRE is tasked by CMS to perform an application-only scope SCA in accordance with the *CMS Information Security (IS) Authorization to Operate Package Guide, v2.0*[1] for the HIX's available modules that have not previsouly undergone a Security Controls Assessment(SCA) located at the located at the (b)(5), (b)(6), (b)(7)c, (b)(7)e (b)(5), (b)(6), (b)(7)c, (b)(7)e he SCA complies with federal standards, policies, and procedures including the Federal Information Security Management Act of 2002 (FISMA) and the security-related areas as established and specified by the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Rev. 3, *Recommended Security Controls for Federal Information Systems and Organizations*[2] and the mandatory, non-waiverable Federal Information Processing Standards (FIPS) 200, *Minimum Security Requirements for Federal Information and Information Systems.*[3]

To comply with the federal standards, agencies must first determine the security category of their information system in accordance with the provisions of FIPS 199, *Standards for Security*

[1] http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/ATO_Package_Guide.pdf

[2] http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf.

[3] http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf.

Categorization of Federal Information and Information Systems,[4] and then apply the appropriate set of minimum (baseline) security controls in compliance with the NIST SP 800-53. Furthermore, CMS developed and published the *Information Security (IS) Acceptable Risk Safeguards (ARS) including CMS Minimum Security Requirements (CMSR) Version 1.5*,[5] *CMS Policy for Information Security Program (PISP)*,[6] and *Business Partners Systems Security Manual Version 10.0 (BPSSM)*.[7] The CMS ARS CMSR contains a broad set of required security standards based upon NIST SP 800-53 and NIST 800-63, *Electronic Authentication Guideline*[8] as well as additional standards based on CMS policies, procedures and guidance, other federal and non-federal guidance resources, and industry best practices. To protect CMS information and CMS information systems, the controls outlined in these policies must be implemented.

1.3 Assessment Process and Methodology

This section outlines MITRE's assessment methodology to verify and validate that the management, operational, and technical controls are appropriately implemented.

1.3.1 Phase 1: Planning

The first phase, "Planning", defines the assessment's scope, identifies goals, sets boundaries, and identifies assessment activities. This phase, as well as subsequent phases, requires the coordination of all involved parties, including CMS, MITRE, and CGI Federal. During this phase, the MITRE Evaluation Team will review all security policies and procedures in accordance with CMS security requirements as previously noted. The team will then create assessment scenarios and premises and define agreeable assessment terms as approved by CMS.

1.3.2 Phase 2: Assessment

Phase 2 may have several steps depending on the assessment's objectives, scope, and goals as set forth in the Planning Phase. These steps can be grouped by the nature of the activities involved. These activity groups are as follows:

- Information Collection—thorough research that must be performed against the target system/application before any meaningful assessment can be conducted. Data gathered is analyzed as the assessment proceeds and when the assessment is complete.
- Enumeration—activities that provide specific information about assessment targets. This information is often collected using appropriate software tools.
- Testing and Review—activities that typically involve both the automated testing of security vulnerabilities via software tools, manual analysis, and the evaluation of particular aspects of the organization's security policies and practices by the MITRE Evaluation Team members. MITRE's evaluation goal is to apply experience and insight in order to determine

[4] http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf.

[5] ARS CMSR Version 1.5 (July 31, 2012) at https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html.

[6] http://www.cms.hhs.gov/informationsecurity/downloads/PISP.pdf

[7] http://www.cms.gov/manuals/downloads/117_systems_security.pdf (July 17, 2009).

[8] http://csrc.nist.gov/publications/nistpubs/800-63-1/SP-800-63-1.pdf.

whether the system adequately implements security controls defined by CMS policies and standards.

1.3.3 Phase 3: Reporting

Phase 3, "Reporting", documents the soundness of the implemented security controls and consolidates all findings into the final output. This output includes reports that provide a summary of key findings and actionable recommendations, as well as provisions for all information derived from the assessment.

Depending on the results of these activities, it may be necessary to repeat appropriate phases. Throughout the entire process, the MITRE Evaluation Team will keep all involved parties informed of the progress and findings, as well as provide briefings of findings to CMS and CGI Federal staff. Evidence to support any weaknesses discovered will consist primarily of screen prints, script output, and session data. MITRE will immediately notify CMS and CGI Federal staff if significant or immediately exploitable vulnerabilities are discovered during the assessment.

2 PLANNING

This section contains information describing the modules, sometimes referred to as "applications", and environment that will be assessed, the scope of the assessment, any limitations, and roles and responsibilities of staff who will participate in the assessment.

2.1 PLAN MANAGEMENT BACKGROUND

Plan Management

The Plan Management (PM) Qualified Health Plan (QHP) Issuer Certification module of the Federally Facilitated Marketplace (FFM) is a means for the Issuers, States, and the Centers for Medicare and Medicaid Services (CMS) to enter data that can later be used for displaying the plans and benefits for consumers.

The PM business area consists of business processes for acquiring, certifying, monitoring, renewing, and managing the withdrawal of qualified health plans (QHPs) and the Issuers that offer these plans for a given Marketplace. These areas are currently supported by a composite solution consisting of:

- Data submission templates (MS Excel-based) allowing States and Issuers or their representatives to download, populate, validate, and upload into the PM system various complex data sets detailing application, plan, and rate and benefits information.
- User interfaces and services for State and Issuer users to submit, review, modify, and attest to the information uploaded or provided directly via the user interface to support the application and rate and benefits collection process for a given Exchange or set of Exchanges.
- User interfaces and services for CMS personnel to review, monitor, and certify/decertify applications and plans submitted for approval in a given Exchange.
- System interfaces to existing CMS systems (e.g., HIOS) to support streamlined data and profile collection and authentication.
- A system interface to CMS's PDF generation solution, (b)(5), (b)(6), (b)(7)c, (b)(7)e (b)(5), (b)(6), (b)(7)c, (b)(7)e for creation of notices that are distributed to Issuers.

The Plan Preview module provides Issuers with the capability to view rates and plan details based on a set of subscriber and plan variance data selected by the user. The Summary page provides the user with the ability to select a specific IssuerID to preview their plan(s). The user can view an Issuer's submitted plans and rating scenarios by clicking on the View Plans button that corresponds to an Issuer in the Issuer table. The Rating Scenarios page allows the user to select plans and various inputs necessary for the rating engine to provide a rate(s).

2.2 ASSESSMENT SCOPE

MITRE is tasked with providing an application-only SCA to determine if the HIX updates have properly implemented CMS security standards. According to the System Security Plan (SSP), the FIPS 199 security categorization level for the HIX is Moderate since HIX contains sensitive information about persons and sensitive documents from insurance companies. The SCA will examine the management, operational, and technical controls that support the HIX updated Modules listed below to ensure adherence to the Moderate security level specifications in the CMS ARS CMSR, PISP, and BPSS,. To adequately perform the SCA, MITRE anticipates that the MITRE Evaluation Team will be onsite for five days from August 19-30, 2013.

2.2.1 Database Testing:

All data collected is stored in the (b)(5), (b)(6), (b)(7)c, (b)(7)e and the (b)(5), (b)(6), (b)(7)c, (b)(7)e system.

- MITRE requires the information and knowledge transfer from CMS and CGI Federal concerning the PM Module database(s) and instances. MITRE will work with CGI Federal to assemble a plan to test the database(s) in scope for the SCA. A database build document, security version description document, and System Design document would enhance the preparation for MITRE to test the PM Module database(s).
    - A separate Database Interview for the SCA will not be necessary since the database administration has been previously assessed in prior SCA's. Reporting of findings will occur in the SCA's Daily out-briefs and if common with previous platform findings, then those findings will be classified as "informational only".

Application testing will be performed in vairous environments, see chart below, and in adherence to the *CMS Information Security (IS) Assessment Procedure Version 2.0*[9] that establishes a uniform approach for the conduct of IS testing of the CMS Information Systems for major applications and their underlying component application systems. The following CMS ARS CMSR security control families will be the focus for testing:

Application Only Scope SCA:

- Access Control (AC), all controls except AC-1, AC-18, AC-19, and AC-20
- Awareness and Training (AT), only AT-2 and AT-3
- Audit and Accountability (AU), all controls except AU-1
- Security Assessment and Authorization (CA), all controls except CA-1
- Configuration Management (CM), all controls except CM-1
- Contingency Planning (CP), all controls except CP-1, CP-6, CP-7, CP-8, and CP-9
- Identification and Authentication (IA), all controls except IA-1, and IA-3
- Maintenance (MA), only MA-3
- Media Protection (MP), only MP-5 and MP-6
- Physical and Environmental (PE), only PE-2, PE-5, and PE-17
- Planning (PL), all controls except PL-1 and PL-4
- Personnel Security (PS), all controls except PS-1, PS-2, PS-3, and PS-8
- Risk Assessment (RA), only RA-2 and RA-3
- System and Services Acquisition (SA), all controls except SA-1, SA-7, and SA-9
- System Communications (SC), all controls except SC-1, SC-4, SC-12, SC-17, SC-20, SC-21, SC-22, and SC-32
- System and Information Integrity (SI), all controls except SI-1, SC-3, SI-5, and SI-8

[9] http://www.cms.hhs.gov/informationsecurity/downloads/Assessment_Procedure.pdf (March 19, 2009).

The following table represents the functionality that will be tested per module. The table also details the testing environment by name, when testing may be performed and if/when a demo/walkthrough may be performed.

Module Name	Functionality	Is UI present – if no, to be tested by (b)(5), (b)(6), (b)(7)c, (b)(7)e Messaging	SCA Testing Environment	Date available in intended SCA testing environment	Date available to demo
PM	Plan Transfer	No	(b)(5), (b)(6), (b)(7)c, (b)(7)e	Now	8/19 - no formal demo; background process walkthrough
	Plan Preview	Yes	(b)(5), (b)(6), (b)(7)c, (b)(7)e	8/15	Now
	Plan Ratification, Certification, and Accreditation (includes Plan Confirmation)	Yes	(b)(5), (b)(6), (b)(7)c, (b)(7)e	8/24	8/24
	Certification Notices	No	(b)(5), (b)(6), (b)(7)c, (b)(7)e	8/24	8/19 - no formal demo; background process walkthrough
FM	SBM Data Collection and Validation	No	(b)(5), (b)(6), (b)(7)c, (b)(7)e	8/15	8/15
	Preliminary CSR Calculation	No	(b)(5), (b)(6), (b)(7)c, (b)(7)e	8/15	8/15
E&E	(b)(5), (b)(6), (b)(7)c, (b)(7)e	Yes	(b)(5), (b)(6), (b)(7)c, (b)(7)e	8/19	8/7
	My Account	Yes (with known limitations and omissions)	(b)(5), (b)(6), (b)(7)c, (b)(7)e	8/16	8/19

Module Name	Functionality	Is UI present – if no, to be tested by SOAP services Messaging	SCA Testing Environment	Date available in intended SCA testing environment	Date available to demo
	Individual Application	Yes (with known limitations and omissions)	(b)(5), (b)(6), (b)(7)c, (b)(7)e	8/16	8/19
	Direct Enrollment	Yes	(b)(5), (b)(6), (b)(7)c, (b)(7)e	8/16	8/19
	Plan Compare	Yes (with known limitations and omissions)	(b)(5), (b)(6), (b)(7)c, (b)(7)e	8/16	8/19

2.3 Limitations and Omissions

2.3.1 My Account Known

- LOA2 Step-up functionality is not yet available
- Final profile landing page and features (such as application history, plan selection, etc.) is not available
- Ability to edit an existing application is not yet available
- Landing pages for non-Consumers (e.g., Agent/Brokers, CCRs) are not yet available

2.3.2 Individual Application

- Specific data sets (e.g., Mathematica data) must be used to get through the application correctly to match the staged data by the Data Services Hub
- Getting Started section
  - Household contact will be editable – info does not currently import from My Account
- Additional Information section
  - Stubbed Non-ESC insurance pages – the final pages to collect this data are not yet available
- Eligibility Results Page
  - Final page design is not yet available
- Using stubbed MaxAPTC service in (b)(5), (b)(6), (b)(7)c, (b)(7)e to defects is still being resolved in lower environments

2.3.3 Plan Compare

- (b)(5), (b)(6), (b)(7)c, (b)(7)e [redacted] there is a temporary passcode page to protect non-certified plans from being viewed by non-authorized personnel. This page will not be part of the 10/1 code base. The Passcode can be obtained directly from Mark Oh.
- Individual Application and Plan Compare modules are not linked (e.g., a user cannot yet seamlessly navigate from one to the other). Once eligibility results are obtained and an application ID is returned to the user, the tester must currently enter a new URL directly to navigate to the Plan Compare passcode page (mentioned above) and enter the passcode and application ID to proceed to the Plan Compare pages and be able to return plan data back to the user.
- Multiple tax households is not supported at this time
- Multi-filter is not currently working

2.4 Assessment Assumptions/Limitations

MITRE has identified limitations of the planned assessment:

- The (b)(5), (b)(6), (b)(7)c, (b)(7)e [redacted] is in scope, as it has been altered from the previous assessment.
- The (b)(5), (b)(6), (b)(7)c, (b)(7)e [redacted] is not in scope.
- (b)(5) [redacted]
- (b)(5) [redacted]
- The application modules being tested is functionally equivalent to the application deployed in the production environment.
- CGI Federal staff will provide timely responses to MITRE requests for information, access to systems to perform application testing and CGI Federal subject matter experts as documented in the SCA test plan.
- All the policies and procedure that govern the testable modules are the same policies and procedures that were assessed as part of the HIX/QHP assessment March-April 2013. Therefore, the policies and procedures will not be assessed, the documents SSP, ISRA and CP will be evaluated due to significant updateds.
- Findings remediation for previously assessed modules (Operating System, Database and Applciations) are considered to be secondary and may be reevaluated if time and resources permit..
- Code Changes, hot fixes, patches etc. will be made known to MITRE via email PRIOR to the change being performed, followed by the documented authorization for the change, which states what the change was and who authorized it.
- Test Data will be prepopulated by CGI Federal for some test accounts.
- No application interviews will be formally scheduled. Ad-Hoc application interviews may be performed as needed and agreed upon by MITRE and CGI Federal.

2.5 Data Use Agreement

The Data Use Agreement (DUA), form CMS-R-0235, must be executed prior to the disclosure of data from the CMS Systems of Records to ensure that the disclosure will comply with the requirements of the Privacy Act, Privacy Rule, and CMS data release policies. It must be completed prior to the release of, or access to, specified data files containing protected health information (PHI) and individual identifiers. MITRE has completed and signed this agreement with CMS Reference DUA number 19317; expiration date October 20, 2013.

2.6 Roles and Responsibilities

To prepare for the assessment, the organization(s) and MITRE will identify personnel associated with specific responsibilities. Individuals may have responsibilities that span multiple roles or have knowledge pertaining to the implementation of more than one security control area. This section provides a description of the roles and responsibilities to assist the organization(s) and MITRE in determining the appropriate personnel who should be available for the assessment.

2.6.1 Application Developer/Maintainer

The Application Developer/Maintainer shall have a thorough knowledge of the application security control requirements for the system and their implementation to protect the software application, its data in transit and at rest, as well as the implementation and configuration standards utilized by the organization. These controls may include access control, audit and accountability, user identification and authentication, software code configuration control, application integrity, and communications protection. During the SCA process and onsite assessment, the Application Developer/Maintainer shall be available for planning sessions, interviews, application discussions, providing assistance for using the application, providing documentation under their control, and remediating any weaknesses.

2.6.2 Business Owner

The Business Owner is responsible for the successful operation of the system and ultimately accountable for system security. The Business Owner defines the system’s functional requirements, ensures that Security Accreditation (previously referred to as Certification and Accreditation [C&A]) activities are completed, maintains and reports on the Plan of Action & Milestones (POA&M), and ensures that resources necessary for a smooth assessment are made available to the MITRE Evaluation Team (Assessment Contractor). During the SCA process and onsite assessment, the Business Owner shall be available for planning sessions, interviews, system discussions, providing documentation, and providing assistance when necessary (access, contacts, decisions, etc.) In some cases the Business Owner may be the System Owner.

2.6.3 CMS Facilitator

The CMS Facilitator is a member of the CMS SCA Team staff responsible for scheduling and communicating information on all planning and coordinating meetings as well as out-briefs associated with the SCA. The CMS Facilitator reserves work space for testing when the tests are conducted at CMS facilities. In addition, the CMS Facilitator coordinates the logistics between the CMS SCA Team and SCA Stakeholders (application developers, maintainers, technical support, business owners, etc.) The CMS Facilitator is responsible for initiating application and system access for the test accounts used during the assessment. At the conclusion of the assessment, the CMS Facilitator accepts the Security Controls Assessment Report, distributes the final report to SCA Shareholders and generates the cover letter associated with it.

2.6.4 CMS Government Task Lead

The CMS Government Task Lead (GTL) is a CMS representative for the Application Developer/ Maintainer and is responsible for providing technical information to the SCA Team. During the SCA process and onsite assessment, the GTL shall be available for planning sessions, interview with their Application Developer/ Maintainer, assisting the Application Developer during application discussions, providing assistance for using the application, and directing the Application Developer/Maintainer to remediate any weaknesses.

2.6.5 Database Administrator

The Database Administrator(s) shall have a thorough knowledge of the database software and the databases that support the system, as well as the implementation and configuration standards utilized by the organization for the software and databases. The Database Administrator shall be able to describe the processes and procedures for installing, supporting, and maintaining the database software and databases, including secure baseline installation, access control, identification and authentication, backup and restoration, and flaw remediation. During the SCA process and onsite assessment, the Database Administrator shall be available for interview, database discussions, execution of scripts to collect configuration details, providing documentation when necessary, and remediation of any weaknesses.

2.6.6 Information System Security Officer or System Security Officer

The Information System Security Officer (ISSO) or System Security Officer (SSO) is responsible for ensuring that the management, operational, and technical controls to secure the system are in place and effective. The ISSO shall have knowledge of the following:

- All controls implemented or planned for the system
- Security audit controls and evidence that audit reviews occur
- System Security Plan (SSP) and any authorized exceptions to security control implementations

The ISSO shall be responsible for all security aspects of the system from its inception until disposal. During the SCA process and onsite assessment, the ISSO plays an active role and partners with the CMS Facilitator to ensure a successful SCA. The ISSO shall be available for interview, provide or coordinate the timely delivery of all required SCA documentation; and coordinate and schedule interviews between the SCA Team and SCA Stakeholders. The ISSO is designated in writing and must be a CMS employee.

2.6.7 Lead Evaluator

The Lead Evaluator is a member of the MITRE Evaluation Team and responsible for understanding CMS policies, standards, procedures, system architecture and structures. The Lead Evaluator has limited activities within the SCA scope; reports all vulnerabilities that may impact the overall security posture of the system; refrains from conducting any assessment activities that she/he is not competent to carry out or to perform in a manner which may compromise the information system being assessed; and coordinates getting information, documentation and/or issues addressed between the MITRE Evaluation Team, the CMS Facilitator, and the SCA Stakeholders. The Lead Evaluator must develop the *Assessment Plan;* modify the testing approach, when necessary according to the scope of the assessment; prepare the daily agenda, preliminary findings worksheets and conduct the Onsite Assessment briefings; and prepare a Security Controls Assessment Report (e.g., Findings Report) to communicate how the CMS business mission will be impacted if an identified vulnerability is exploited.

2.6.8 Program Manager

The Program Manager shall have a high-level understanding of the assessed system, as well as the ability to describe organizational and system policies from an enterprise perspective, with which the system shall be in compliance. The Program Manager shall be familiar with access controls, both physical and logical, contingency plans (i.e., alternate sites/storage, system restoration and reconstitution), user identification and authentication, system authorization to operate, incident response, resource planning, system and software acquisition, flaw remediation, and system interconnections and monitoring. During the SCA process and onsite assessment, the Program Manager shall be available for interview and to provide documentation that falls under the Program Manager's responsibility.

2.6.9 System Administrator

The System Administrator(s) should have a thorough knowledge of the operating systems for which they are responsible, as well as the implementation and configuration standards utilized by the organization for those operating systems. The System Administrator (s) should be able to describe the processes and procedures for installing, supporting, and maintaining the operating systems, including secure baseline installation, access control, identification and authentication, backup and restoration, flaw remediation, and use of antivirus products. During the assessment, the System Administrator (s) should be available to establish access to the system, interviews, system discussions, execution of scripts to collect configuration details, and remediation of any weaknesses found that could be corrected within the assessment timeframe.

2.6.10 System Owner

The System Owner is responsible for the successful operation of the system and accountable for system security. The System Owner is also responsible for executing crucial steps to implement management and operational controls and to ensure that effective technical controls are implemented to protect the system and its data. The System Owner formally designates the ISSO. In conjunction with the Business Owner, the System Owner is responsible for ensuring that Security Accreditation activities are completed and the POA&M is maintained and reported. During the SCA process and onsite assessment, the System Owner shall be available for interview and, with the assistance of the system's support staff, ensure that all documentation required for the assessment is available to the SCA Evaluator. The System Owner may be the Business Owner.

2.7 Assessment Responsibility Assignment

For this assessment, MITRE, CMS, and CGI Federal staff names have been associated with the specific roles and corresponding responsibilities. The Business Owner may delegate their responsibilities during the engagement, but the name of the delegated individual should be updated in Table 1, which provides details on the responsibilities for the assessment based on the identified roles and responsibilities provided in the preceding Section, "Roles and Responsibilities."

Table 1. Assessment Responsibilities

Name	Organization	Role
Kirk Grothe	CMS/OIS/CIISG	Application Developer
Jim Kerr	CMS/OIS/CIISG	Business Owner
Darrin Lyles	CMS/OIS/CIISG	CMS Facilitator (Lead)
Mark Oh	CMS/OIS/CIISG	CMS Government Task Leader
Joe (Zhengyu) Zhu	CGI Federal	Database Administrator
Tom Schankweiler Darrin Lyles	CMS/OIS CMS/OIS	SSO ISSO
Jim Bielski	MITRE	Project Lead
Jim Huff	MITRE	Lead Evaluator
Mark Calem	CGI Federal	Project Manager
Monica Winthrop	CGI Federal	Deputy Project Manager
Patrick Bruszewski	CGI Federal	System (b)(5), (b)(6), (b)(7)c, (b)(7)e
Rich McCoy	CGI Federal	Plan Management Release Manager
Keith Rubin	CGI Federal	Chief Architect
Balaji Ramamoorthy	CGI Federal	Senior Security Architect
Raj Sundar	CGI Federal	Security Architect
Joel Singer	CGI Federal	Infrastructure Manager
Patrick Bruszewski	CGI Federal	Infrastructure Configuration Manager
Patrick Bruszewski	CGI Federal	Infrastructure Engineer

2.8 Physical Access and Work Area Requirements

MITRE will require access to various systems, networks, infrastructure, and facilities. The MITRE Evaluation Team will require direct network connectivity to CGI Federal servers and also network access to the Internet. A work area for these individuals needs to be established and include power, table, and chairs. In addition, MITRE staff will require a work area for conducting interviews and analyzing data. CGI Federal will reserve appropriate facilities for the MITRE Evaluation Team while onsite.

3 ASSESSMENT

This section contains information describing the activities to be performed during the assessment for information collection, enumeration, testing and review.

3.1 INFORMATION COLLECTION

MITRE will require access to documentation, operating system and network configuration data, and application information in order to begin the assessment.

3.1.1 CMS FISMA Controls Tracking System (CFACTS) Name

To ensure that the final security controls/ findings worksheet can be properly loaded in to the CMS FISMA Controls Tracking System (CFACTS) at the end of the assessment MITRE must have the correct system name as contained within CFACTS. This system name will be used to correctly populate the System Name field in the Final Management Worksheet delivered with the Final Report.

CFACTS System Name
HIX

3.1.2 Documentation Requirements

MITRE must obtain the documentation requested one week prior to the onsite Assessment "Kick-off" meeting. In order to effectively perform the assessment and prevent delays during the SCA, MITRE must receive the following information that pertains to the application and/or system under evaluation prior to arriving onsite. Failure to receive this information in a timely manner will impact the assessment's quality and MITRE's ability to determine whether management, operational, and technical controls have been implemented properly. To assist MITRE in determining the completeness of this information and serve as a checklist, CMS and CGI Federal should use Tables 2–5 as guides and include any comments that may be applicable (e.g., new system being accredited, no SSP Accreditation Form provided, Configuration Management Plan included in SSP, server Internet Protocol (IP) addresses, and network diagram included in the System Design Document [SDD]). The documentation is broken into four categories:

- Mandatory Pre-Assessment Documentation
- Documentation Required by Policy (e.g., PISP or Integrated IT Investment and System Life Cycle Framework [Integrated Life Cycle (ILC) Framework])
- Expected/Supporting Documentation
- Additional Documentation

Mandatory Pre-Assessment Documentation: The documents in Table 2. Mandatory Pre-Assessment Documentation should be provided within a week after the preliminary call (or within the agreed upon timeframes as noted in the preliminary call meeting minutes) for use in the development of the draft test plan. These can be draft documents if necessary, but "final versions" must be provided at least one week prior to the on-site assessment. Failure to receive these documents could affect the quality of the assessment and would be an ineffective and inefficient use of funds for the assessment to continue. Starting in August, 2012, there may also be additional funding required before the onsite testing can proceed if all requirements are not addressed prior to the scheduled testing date. However, there may be special cases in which CMS wants the evaluator to proceed without all of the documentation, such as a FISMA one-third SCA or if CMS believes a project/system/application is placing CMS at such a great risk that funding may be pulled. For the latter, CMS will request the evaluator's advice on the risk that is posed.

Table 2. Mandatory Pre-Assessment Documentation

Document Element #	Document/Information Requested	ARS CMSR	Policy	Comments
D01	Information System Risk Assessment (IS RA)	RA-3 Risk Assessment	ILC Framework CMS PISP CMSR	G.Cauldfield/ CGI Federal 08/12/2013 CALT doc43385
D02	System Security Plan (SSP) SSP Workbook	PL-2 System Security Plan CA-4 Security Certification	ILC Framework CMS PISP FISMA CMSR	G.Cauldfield/ CGI Federal 08/12/2013 CALT doc42491 & doc42493
D03	Privacy Impact Assessment (PIA)	PL-5 Privacy Impact Assessment	ILC Framework CMSR	G.Cauldfield/ CGI Federal 08/12/2013 CALT doc43900
D04	Contingency Plan	CP-2 Contingency Plan	ILC Framework CMSR	G.Cauldfield/ CGI Federal 08/12/2013 CALT doc43901
D05	**Uniformed Resource Locators (URL) to all Web application interfaces within scope of assessment, if not documented in the SDD, VDD, or SSP)**	SA-5 Information System Documentation	CMSR	

Documentation Required by Policy: CMS Policy requires that a system or application have the following documents listed in Table 3. The absence of these documents is handled in a uniform manner. For example, if policy requires document D12, Baseline Security Configurations, be completed and it does not exist, the absence of the document will result in a finding, assuming the security control is in scope for the assessment.

Table 3. Documentation Required by Policy

Document Element #	Document/Information Requested	ARS CMSR	Policy	Comments
D06	**System Design Document (SDD)**	SA-3 Life Cycle Support	ILC Framework CMSR	G.Cauldfield/ CGI Federal 08/12/2013 CALT doc42632, doc42756, and doc38859
D07	**Version Description Document (VDD)**	SA-3 Life Cycle Support	ILC Framework CMSR	G.Cauldfield/ CGI Federal 08/12/2013 CALT doc42679,

Document Element #	Document/Information Requested	ARS CMSR	Policy	Comments
				doc42727, and doc39345
D08	Interconnection agreements, Memorandum of Understanding (MOU) and/or Interconnection Security Agreement (ISA)	CA-3 Information System Connections SA-9 External Information System Services	CMSR	
D09	RoB. Included evidence that RoBs have been acknowledged//signed by users	PL-4 Rules of Behavior	CMSR	
D10	Contingency Plan Test	CP-4 Contingency Plan Testing and Exercises	ILC Framework CMSR	not completed as of 8/12/2013
D11	Configuration and change management process. Include examples of change requests (CR) from request to implementation in production	CM-3 Configuration Change Control CM-4 Monitoring Configuration Changes CM-5 Access Restrictions for Change	CMSR	G.Cauldfield/ CGI Federal 08/12/2013 CALT doc43904
D12	**Baseline security configurations for each platform and the application within scope and baseline network configurations**	CM-2 Baseline Configuration CM-6 Configuration Settings	CMSR	G.Cauldfield/ CGI Federal 08/12/2013 CALT doc43904
D13	Security awareness and training (AT) material including evidence of staff who have completed training	AT-1 Security Awareness and Training Policy and Procedures AT-2 Security Awareness AT-3 Security Training AT-4 Security Training Records AT-5 Contacts with Security Groups and Associations	CMSR	G.Cauldfield/ CGI Federal 08/12/2013 CALT doc24409, doc24406, doc24407, and doc24405
D14	Incident response (IR) procedures. Include evidence of simulations or actual execution of IR procedures	IR-1 Incident Response Policy and Procedures IR- 2 Incident Response Training IR- 3 Incident Response Testing and Exercises IR- 4 Incident Handling IR- 5 Incident Monitoring IR- 6 Incident Reporting IR- 7 Incident Response Assistance	CMSR	N/A, inherited control from PaaS
D15	**Documentation describing the types of audit logging that is enabled and the established rules for log review and reporting**	AU-6 Audit Monitoring, Analysis, and Reporting	CMSR	N/A, inherited control from XOC and (b)(5), (b)(6), (b)(7)c, (b)(7)e
D16	Open Corrective Action Plans	CA-5 Plan of Action and	CMSR	G.Cauldfield/ CGI

Document Element #	Document/Information Requested	ARS CMSR	Policy	Comments
	(CAP) items from previous security controls assessments	Milestones (POA&M)		Federal 08/12/2013 CALT doc44070
D17	System of Record Notice (SORN)	PL-5	ILC Framework CMSR	See the Master Helath Insurance Exchange SORN 09-70-0560

Expected/Supporting Documentation: Table 4 provides a list of other supporting documents that are applicable to an application or system. Although these documents are not specifically required by security policy, the documents should exist based on the CMS ILC and should be provided to MITRE during the assessment as they may be helpful in performing the assessment, determining any special circumstances or permissions that vary from the CMS standards and also used as substantiating artifacts.

Table 4. Expected/Supporting Documentation

Document Element #	Document/Information Requested	ARS CMSR	Policy	Comments
D18	**Operations & Maintenance (O&M) Manual**	SA-5 Information System Documentation	ILC Framework CMSR	If databases and servers are in scope
D19	Application or system (depending on assessment's scope) backup and storage requirements and procedures. In addition, include data retention and media handling/sanitization procedures	CP-6 Alternate Storage Site CP-9 Information System Backup MP-4 Media Storage MP-6 Media Sanitization and Disposal	CMSR	N/A
D20	Detailed system/network architecture diagrams with IP addresses of devices that will be within scope of assessment, if not documented in the SDD, VDD, or SSP)	SA-5 Information System Documentation	CMSR	May be documented in the SSP
D21	Security *processes*, including application account creation and account review policy, password policy and malicious, mobile code, and antivirus policy. For password management, ensure policies cover both end user access as well as user accounts used for production operations	AC-1 Access Control Policy and Procedures IA-1 Identification and Authentication Policy and Procedures	CMSR	IN SSP
D22	CMS Security Certification Form (if system previously authorized—TAB A)	CA-6 Security Authorization	CMSR	N/A

Document Element #	Document/Information Requested	ARS CMSR	Policy	Comments
D23	Technical Review Board (TRB) and TRA letters to include all PDR, DDR and ORR documentation. Primarily for major updates and new applications	CM-3 Configuration Change Control	CMSR	Required to determine variances from the CMS Policies and Standards

Additional Documentation: Additional documentation in Table 5 may be requested during the assessment, depending on the system/application being assessed.

Table 5. Additional Documentation

Document Element #	Document/Information Requested	ARS CMSR	Policy	Comments
D24	**Administrator/Operator and User manuals or training materials, if not documented in the SDD, VDD, or SSP)**	SA-5 Information System Documentation	ILC Framework CMSR	Application Walkthrough and supplemental documentation to assist understanding of PM Module testing.

3.1.3 Script Output Configuration Requirements

MITRE must obtain the database , one week prior to the onsite assessment Kick-off meeting. Having the script output prior to the onsite assessment enables MITRE to immediately begin reviewing configuration settings and identifying areas that may require further analysis. Failure to receive the output prior to the MITRE Evaluation Team arriving onsite will impact the assessment's quality and MITRE's ability to determine whether management, operational, and/or technical controls have been implemented properly. "As Is" system implementation documentation, including build documents and configuration scripts for servers, will be collected and analyzed.

3.1.4 Application Testing Requirements

In order to test the HIX/QHP Plan Management Module application, accounts that reflect the different user types and roles need to be created and tested prior to MITRE arriving onsite. MITRE requires that application-specific user accounts be created for MITRE Evaluation Team members as authorized by CMS. This will enable MITRE to test application security controls and environment vulnerabilities. ***Application access allocations for the test accounts must be completed two weeks prior to the onsite assessment kick-off meeting and communicated to MITRE, so where possible, MITRE may confirm that the accounts can login to the application.***

Table 6. Application Roles

Role	Description	Privileges
Administrator	Administers access control and security functions for the application	Read, write, and execute for all application data

Role	Description	Privileges
Supervisor	Validates or reviews all user application input	Read, write, and execute for all application data within their role
User	Reads and searches application data	Read all application data within their role

Table 7. Additional Testing Accounts Requirements

Test Account UID	Application Testing Role

3.1.4.1 E&E (b)(5), (b)(6), (b)(7)c, (b)(7)e (Environment: Test1)

URL: (b)(5), (b)(6), (b)(7)c, (b)(7)e

Account Creation: Use the CREATE ACCOUNT button to begin the process. At this point in time, it is acceptable to re-use the same email address for multiple (b)(5), (b)(6), (b)(7)c, (b)(7)e (b)(5), (b)(6), (b)(7)c, (b)(7)e

3.1.4.2 E&E My Account (Environment: (b)(5)

Register a (b)(5) marketplace account (b)(5), (b)(6), (b)(7)c, (b)(7)e

3.1.4.3 E&E Individual Application (Environment: (b)(5))

To access Individual App, create an account. Use the same link to create an account and log in: (b)(5), (b)(6), (b)(7)c, (b)(7)e

3.1.4.4 E&E Plan Compare

Browse to the following URL: (b)(5), (b)(6), (b)(7)c, (b)(7)e

(The state parameter in the URL will need to be changed depending on what state the application was started for).

CMS will provide the Secure Code to MITRE when Plan Compare is ready to be tested.

The application ID from the Individual application or pre-completed applications should be used in the second form field and the popup window after this page.

3.1.4.5 (b)(5)

(b)(5), (b)(6), (b)(7)c, (b)(7)e

User name: (b)(5), (b)(6), (b)(7)c, (b)(7)e
Password:

(b)(5), (b)(6), (b)(7)c, (b)(7)e

The MITRE Team Lead will inform the Business Owner, CMS contractors, and CMS Facilitator when application testing is complete. Following testing, the Business Owner is expected to initiate the process to de-allocate the security access provided to the MITRE test accounts.

3.2 ENUMERATION

MITRE will use various methods and tools to enumerate the system and it security policies.

3.2.1 Vulnerability Assessment Tools

MITRE will work with CMS and CGI Federal staff to verify and determine that industry standard best practices are reflected in the CMS system architecture design. To the extent possible, the work performed on this task will be accomplished on MITRE-furnished auditing equipment. The MITRE Evaluation Team may use the following tools during the assessment:

- **Achilles** (http://www.mavensecurity.com/achilles)—tool designed for testing the security of Web applications
- **Burp Suite** (http://portswigger.net/burp/)—integrated platform for performing security testing of web applications.
- **Cookie Digger** (http://www.foundstone.com)—tool used to collect and analyze cookie values used to maintain session state and isolation through identifying the use of easily guessed or predictable cookie values
- **Curl** (http://curl.haxx.se/)—open-source command line tool for transferring files with Uniformed Resource Locator (URL) syntax
- **Httprint** (http://net-square.com/httprint/)—Web server fingerprinting tool
- **Httrack** (http://www.httrack.com/)—open-source offline browser utility
- **MetaCoretex** (http://sourceforge.net/projects/metacoretex/)—(b)(5), (b)(6), (b)(7)c, (b)(7)e tool that provides a graphical user interface (GUI) and tests a number of different database systems
- **MITRE host-based and database scripts**—scripts developed with the contribution and experience of MITRE's vulnerability and penetration testers. Versions have been developed for both Windows and Unix-based operating systems. With the assistance of System Administrators, the MITRE Evaluation Team uses these scripts to audit operating system security configurations and identify misconfigurations
- **Mozilla and Firefox Web Browsers** (http://www.mozilla.org)—open-source Web-based browsers used to manually browse and inspect the Web application and associated forms
- **Nikto** (http://www.cirt.net/code/nikto.shtml)—open-source, command-line, Web server scanner

- **Nipper Studio** (https://www.titania-security.com/)— software tool that provides comprehensive security auditing and device configuration reporting of network devices, including firewall rule audits and software version vulnerabilities
- **Nmap** (http://www.insecure.org/nmap/)—open-source utility for network exploration or security auditing through UDP and TCP port scanning
- **Paros** (http://www.parosproxy.org)—(b)(5), (b)(6), (b)(7)c, (b)(7)e Web proxy tool used to evaluate Web application security (similar to Achilles)
- **Openssl** (http://www.openssl.org/)—open-source library that provides cryptographic functionality to applications such as secure Web servers
- **SiteDigger** (http://www.foundstone.com/)—tool that searches Google's cache to look for vulnerabilities, errors, configuration issues, proprietary information, and interesting security nuggets on websites
- **SpikeProxy** (http://www.immunitysec.com/resources-freesoftware.shtml)**—**Web proxy that captures and replays Hyper Text Transfer Protocol (HTTP) packets with permuted input
- **Stompy** (http://lcamtuf.coredump.cx)—open-source command line tool (b)(5), (b)(6), (b)(7)c, (b)(7)e is used to collect and analyze cookie and URL parameter values used as session identifiers
- **Stunnel** (http://www.stunnel.org)—universal SSL wrapper that allows the encryption of arbitrary TCP connections inside SSL
- **WebScarab** (http://www.owasp.org/index.php/Category:OWASP_WebScarab_Project)—(b)(5), (b)(6), (b)(7)c, (b)(7)e Web proxy tool used to evaluate Web application security
- **Wget** (http://www.gnu.org/software/wget/wget.html)—open-source network tool that retrieves files from the Internet using HTTP, Secure Hyper Text Transfer Protocol (HTTPS), and FTP protocols
- **Wireshark** (http://www.wireshark.org) – open source, GUI network protocol analyzer

The list above is not all inclusive. MITRE may use other tools and scripts, as needed, and provide test scripts to CMS to share with necessary support staff.

3.3 Testing and Review

MITRE will perform activities that typically involve both the automated testing of security vulnerabilities via software tools, manual analysis, and the evaluation of particular aspects of the organization's security policies and practices.

MITRE will perform the following assessment activities:

- Conduct vulnerability testing with full knowledge of the system, applications, products, configurations, and topology
- Provide MITRE Evaluation Team members, who have specific knowledge of operating systems, firewalls, networking, architecture of transactional Web systems, and Web programming technologies (e.g., Hypertext Markup Language [HTML], (b)(5), (b)(6), (b)(7)c, (b)(7)e Active Server Pages [ASP], cookies, Perl, Common Gateway Interface [CGI], Siebel, WebSphere, and Visual Basic scripting)
- Attempt to gain unauthorized user access or unauthorized access to system resources

- Evaluation of Web application buffer overflow and password vulnerabilities by performing tests that include brute force password attacks and buffer overflow
- Perform application testing to determine if adequate security controls are implemented
- Examine database configuration settings

3.3.1 Interviews

Interviews will focus on a review of the management, operational, and technical controls associated with the CMSR security policies, procedures, and standards. Interviews will also help gain a better understanding of the system environment's security posture and will supplement findings identified during the technical testing. When available and applicable, electronic copies of additional written documentation will be collected for review. Subject matter experts (SME) in the following areas will be interviewed:

- Application Testing

3.3.2 Application Testing

MITRE will test the HIX/QHP Plan Management Module to ensure proper software development techniques, supported software is used, and that the confidentiality, integrity and availability (CIA) of data processed by the application adhere to CMS policies, procedures and standards. Following is a list of activities MITRE will perform:

- Assess if input parameters passed to the application are checked and validated
- Determine if application administrators can remotely access the application via CMS-approved standards
- Examine implemented access control and identification and authentication techniques
- Test to determine if the application is susceptible to (b)(5), (b)(6), (b)(7)c, (b)(7)e (b)(5), (b)(6), (b)(7)c, (b)(7)e or other vulnerabilities
- Examine confidential information to determine if it is encrypted before being passed between the application and browser
- Determine if the application architecture conforms to the TRA

CMS and CGI Federal will provide the appropriate user accounts and logins to access the application to be tested in the targeted environment. The user account logins and application access must be available to MITRE for tests two weeks prior to application testing. At least one account must have administrative access with the ability to adjust the application roles of another login.

3.3.3 Database Server/Instance Testing

MITRE will evaluate database server and software configurations with the help of the appropriate system administrators. MITRE technical staff will work with the system administrators and DBAs to view essential, security-relevant configurations and settings. The following is a list of activities that will be performed:

- Review database security configuration settings to determine if adequate system protections are implemented

THIS PAGE INTENTIONALLY LEFT BLANK

4 REPORTING

This section outlines how MITRE will report vulnerabilities during the assessment.

4.1 Security Controls Assessment Findings Spreadsheet

The SCA findings spreadsheet (Table8) is a running tabulation of possible findings identified during the assessment that is reviewed during daily out-briefs (DOB). Findings are broken out by day and then sorted according to risk level. For updates to a previous day's findings, the updated cell is highlighted in yellow. Although high and moderate risk-level findings are discussed during the DOBs, questions pertaining to low risk-level findings may be raised for clarification. Further details about the spreadsheet columns are listed in the following sections.

(b)(5), (b)(6), (b)(7)c, (b)(7)e

[redacted]

4.1.1 Row Number

Each finding has a row number included to provide easy reference when the spreadsheet is printed and reviewed during DOBs. This row number is also included in the test reports for easy cross reference.

4.1.2 Weakness

A brief description of the security vulnerability is described in the Weakness column.

4.1.3 Risk Level

Each finding is categorized as a business risk and assigned a risk level rating described as high, moderate, or low risk. The rating is, in actuality, an assessment of the priority with which each vulnerability should be addressed. Based on CMS' current implementation of the underlying technology and the assessment guidelines contained with the *CMS Reporting Procedure for Information System (IS) Assessments* document,[10] MITRE will assign these values to each Business Risk. The risk ratings are described in Table9.

Table 9. Risk Definitions

Rating	Definition of Risk Rating
High	Exploitation of the technical or procedural vulnerability will cause substantial harm to CMS business processes. Significant political, financial, and legal damage is likely to result
Moderate	Exploitation of the technical or procedural vulnerability will significantly impact the confidentiality, integrity and/or availability of the system or data. Exploitation of the vulnerability may cause moderate financial loss or public embarrassment to CMS
Low	Exploitation of the technical or procedural vulnerability will cause minimal impact to CMS operations. The confidentiality, integrity and availability of sensitive information are not at risk of compromise. Exploitation of the vulnerability may cause slight financial loss or public embarrassment

4.1.4 CMSR Security Control Family and Reference

The CMSR security control family and control number that is affected by the vulnerability is identified in the CMSR Security Control Family and the Reference columns.

4.1.5 Affected Systems

The systems, URLs, IP addresses, etc., affected by the weakness, are identified in the Affected Systems column.

4.1.6 Ease-of-Fix

Each finding is assigned an Ease-of-Fix rating described as Easy, Moderately Difficult, Very Difficult, or No Known Fix. The ease with which the Business Risk can be reduced or eliminated is described using the guidelines in Table 80.

[10] http://www.cms.hhs.gov/informationsecurity/downloads/Assessment_Rpting_Procedure.pdf.

Table 80. Definition of Ease-of-Fix Rating

Rating	Definition of Ease-of-Fix Rating
Easy	The corrective action(s) can be completed quickly with minimal resources and without causing disruption to the system or data
Moderately Difficult	Remediation efforts will likely cause a noticeable service disruption: • A vendor patch or major configuration change may be required to close the vulnerability • An upgrade to a different version of the software may be required to address the impact severity • The system may require a reconfiguration to mitigate the threat exposure • Corrective action may require construction or significant alterations to the manner in which business is undertaken
Very Difficult	The high risk of substantial service disruption makes it impractical to complete the corrective action for mission critical systems without careful scheduling: • An obscure, hard-to-find vendor patch may be required to close the vulnerability • Significant, time-consuming configuration changes may be required to address the threat exposure or impact severity • Corrective action requires major construction or redesign of an entire business process
No Known Fix	No known solution to the problem currently exists. The Risk may require the Business Owner to: • Discontinue use of the software or protocol • Isolate the information system within the enterprise, thereby eliminating reliance on the system In some cases, the vulnerability is due to a design-level flaw that cannot be resolved through the application of vendor patches or the reconfiguration of the system. If the system is critical and must be used to support on-going business functions, no less than quarterly monitoring shall be conducted by the Business Owner, and reviewed by CMS IS Management to validate that security incidents have not occurred

4.1.7 Estimated Work Effort

Each finding has been assigned an Estimated Work Effort rating described as Minimal, Moderate, Substantial, or Unknown. The estimated time commitment required for CMS or contractor personnel to implement a fix for the Business Risk is categorized in Table 91.

Table 91. Definition of Estimated Work Effort Rating

Rating	Definition of Estimated Work Effort Rating
Minimal	A limited investment of time (i.e., roughly three days or less) is required of a single individual to complete the corrective action(s)
Moderate	A moderate time commitment, up to several weeks, is required of multiple personnel to complete all corrective actions
Substantial	A significant time commitment, up to several months, is required of multiple personnel to complete all corrective actions. Substantial work efforts include the redesign and implementation of CMS network architecture and the implementation of new software, with associated documentation, testing, and training, across multiple CMS organizational units
Unknown	The time necessary to reduce or eliminate the vulnerability is currently unknown

4.1.8 Finding

A detailed description of how the finding did not meet the test description. This provides information on how the actual results fail to meet the security requirement as noted in the CMS security policy, CMS security requirements, CMS guidance or industry best practices published by the Defense Information Systems Agency (DISA) Security Technical Implementation Guides

(STIG), Center for Internet Security (CIS) or database vendors. The finding should have the paragraph from the original report and the date of the final report included in the description as the first line for easy reference in the POA&Ms.

4.1.9 Failed Test Description

The expected results that the finding did not meet are documented. This description provides the specific information from the CMS security policy, requirements, guidance, test objective or published industry best practices.

4.1.10 Actual Test Results

This provides specific information on the observed failure of the test objective, policy or guidance.

4.1.11 Recommended Corrective Actions

The recommended actions to resolve the vulnerability are explained in the Recommended Corrective Actions column.

4.1.12 Status

The Status column provides status information, such as when the vulnerability was identified or resolved.

4.2 Reassignment of Findings

If during the SCA onsite testing period, a finding is determined to be outside the scope of the system or the responsibility of the CMS System Business Owner and ISSO, the finding will be reported and steps should be taken to reassign the finding to the rightful owner. The CMS SCA Facilitator will attempt to contact the rightful owner, provide them with the appropriate information, and invite them to the balance of the SCA proceedings. During the onsite week, the CMS facilitator may assist the CMS System Business Owner and ISSO to obtain the rightful owner's concurrence and responsibility for the finding.

However, it is ultimately the responsibility of the CMS System Business Owner and ISSO to obtain concurrence of the potential finding from the rightful owner and follow through with the necessary reassignment steps prior to the Draft Report Review. If the finding has already been reported in CFACTS, the System Business Owner and ISSO must obtain the CFACTS identifier from the rightful owner and the finding will be closed in the report noting the re-assignment and CFACTS information in the status field. If the ownership of the finding has not yet been successfully re-assigned by the time of the Draft Report Review, the report will be finalized with the finding assigned to the system. It is then the responsibility of the CMS System Business Owner and ISSO to address at a later time and update CFACTS accordingly with the proper information.

Once a finding is reassigned, it should be documented in the system's risk assessment (ISRA). The CMS System Business Owner and ISSO should review periodically as the finding may directly impact the system.

4.3 Reporting Observations

MITRE will include in the finding spreadsheet items that are considered observations instead of actual findings. An observation may arise as a result of a number of situations:

- A security policy or document may be changing and serves to inform the system owner. This gives ample time to prepare for and make appropriate changes;
- A security policy or document has changed and CMS has granted a grace period for completion. The observation provides a mechanism to the business owner/ ISSO that the item requires attention before the end of that grace period;
- A possible finding that the Security Assessment Contractor may have observed and cannot verify by testing as part of the existing tasking; or
- Issues related to industry "best practices" and that are not identified in the CMS Acceptable Risk Safeguards (ARS) or other guidelines referenced by the ARS. These items are considered "Opportunities for Improvement" (OFI).

The observations will also be included in the SCA report in a separate section. Observations may or may not require additional action of the part of the CMS Business Owner, ISSO or CGI Federal.

4.4 Reporting of (b)(5), (b)(6), (b)(7)c, (b)(7)e Vulnerabilities

Since the first quarter of 2012, (b)(5), (b)(6), (b)(7)c, (b)(7)e attacks have increased almost 70%. (b)(5), (b)(6), (b)(7)c, (b)(7)e vulnerabilities are frequent issues identified in CMS System Security Controls Assessments. The Chief Information Security Officer (CISO) and the Enterprise Information Security Group (EISG) considers all (b)(5), (b)(6), (b)(7)c, (b)(7)e vulnerabilities discovered in CMS systems to be rated as a HIGH risk finding whether or not the system is Internet facing.

4.5 Test Reporting

MITRE will also conduct a final out-brief, if needed, after the onsite assessment is completed. Typically, MITRE does not have the opportunity to review all the documentation, configurations, and script outputs while onsite and will need additional days to finish identifying potential vulnerabilities. If this is the case, CMS will schedule a final out-brief within one week after the onsite assessment is completed.

MITRE will discuss and review all informational evidence of remediated findings that is supplied by CMS, and CGI Federal. The MITRE Evaluation Team will diligently respond to inquiries made by CMS, and CGI Federal concerning the validity of findings and acknowledge any areas of concern that may occur. The substance of evidence will contain any mitigation proof reflective of, and as close to, the source of the impacted system as possible. The manner of evidence exchange will be tracked and protected by the MITRE Team Lead, GTL, CMS Facilitator and authorized Points of Contact (POC) for the system(s) tested. ***If CMS authorizes the submission of remediation evidence after the onsite dates, the focus should be on addressing High and Moderate risk findings. In order to promptly meet schedules, MITRE requests that all evidence of remediated findings be submitted to MITRE by the due date established by CMS. This is typically one week after the final out-brief.***

Approximately three weeks following the final out brief, MITRE will provide a draft test report. The test report takes the vulnerabilities identified in the findings spreadsheet and reformats and sorts the information to conform to CMS guidelines contained within the *CMS Reporting Procedure for IS Assessments* document. CMS and CGI Federal will be provided approximately one week to review the test report. Following a draft test report review conference call that will be scheduled by CMS, MITRE will generate a final test report and a data worksheet. The data worksheet will contain all findings not closed during the onsite or the remediation period following the assessment.

5 LOGISTICS

5.1 POINTS OF CONTACT

The MITRE POCs for the SCA are listed in Table 102.

Table 102. MITRE Evaluation Team Points of Contact

Name	Position	Phone Number	Email Address
Jim Huff	Lead Evaluator	(410) 402-2719	jhuff@mitre.org
Chriss Koch	Application Evaluator	(719) 572-8223	cgk@mitre.org
Cheryl Zobel	Application Evaluator	(703) 983-5174	czobel@mitre.org
Mehdi Sayed	Application Evaluator	(410) 303-1273	msayed@mitre.org
Harvey Rubinowitz	Database Evaluator	(781) 271-3076	hhr@mitre.org
Liz Brown	Documentation Evaluator-	(703) 983-1421	ebrown@mitre.org

During assessments, testing problems may be encountered outside normal working hours and require that staff need to be contacted. The CMS POCs for the SCA are listed in Table 113.

Table 113. CMS Points of Contact

Name	Position	Phone Number	Email Address
Tom Schankweiler	CMS/OIS Facilitator	(410) 786-5956	thomas.schankweiler@cms.hhs.gov
Darrin Lyles	CMS/OIS Facilitator	(410) 786-4744	darrin.lyles@cms.hhs.gov
Kirk Grothe	CMS Maintainer	(301) 492-4377	kirk.grothe@cms.hhs.gov
Jim Kerr	Business Owner	(301)-492-4376	james.kerr@cms.hhs.gov
Mark Oh	GTL	(301) 492-4378	mark.oh@cms.hhs.gov

The CGI Federal POCs for the SCA are listed in Table 124.

Table 124. Vendor Points of Contact

Name	Position	Phone Number	Email Address
Lynn Goodrich	Assessment POC and Lead Security Analyst	301-706-9776	lynn.goodrich@cgifederal.com
Greg Caulfield	Secondary Assessment POC and Security Analyst	908-400-1935	greg.caulfield@cgifederal.com
Balaji Ramamoorthy	Lead Security Architect and Primary Technical POC	518-461-9590	balajimanikandan.ramamoorthy@cgifederal.com
Mark Calem	HIX Project Manager	703-227-6921	mark.calem@cgifederal.com

Name	Position	Phone Number	Email Address
Monica Winthrop	HIX Deputy Project Manager	703-227-6012	monica.winthrop@cgifederal.com
Rich McCoy	Plan Management Release Manager	276-889-8854	richard.mccoy@cgifederal.com
Keith Rubin	HIX Chief Architect	973-885-3876	chirayu.desai@cgifederal.com
Joel Singer	IT Operations and Support Manager	703-272-9522	joel.singer@cgifederal.com
Premraj Jeyaprakash	Configuration Manager and System Administrator	703 389 6782	premraj.jeyaprakash@cgifederal.com
Sandeep Johar	Plan Management Technical Lead	571-429-3371	sandeep.johar@cgifederal.com
Pam Rubin	Plan Management Business Requirements Lead	571-533-8605	pamela.rubin@cgifederal.com
Kolap Vanny	Financial Management Release Manager	703-272-6139	kolap.vanny@cgifederal.com
Meg Gill	Financial Management Functional Lead	571-359-7639	marjorie.f.gill@cgifederal.com
Justin Alford	Eligibility & Enrollment Release Manager	571-423-7239	j.alford@cgifederal.com
Vinodh Raman	Individual Appliction POD Lead	571-535-1691	vinodh.raman@cgifederal.com
Ahmad Ramadani	Plan Compare POD Lead	952-393-9068	ahmad.ramadani@cgifederal.com
Steve Wass	My Account POD Lead	301-412-2288	stephen.wass@cgifederal.com
Prabhakar Thopa	Direct Enrollment POD Lead	571-437-9459	prabhakar.thopa@cgifederal.com
Artan Celepia	Plan Management POD Lead	703-966-6255	artan.celepia@cgifederal.com
Rajeev Sood	Financial Management POD Lead	650-201-6318	rajeev.sood@cgifederal.com
Jim Hewitt	HCP BU ISSO and HCSP Director	617-501-7908	james.hewitt@cgifederal.com

5.2 TECHNICAL STAFF REQUIREMENTS

CMS and CGI Federal will need to be available to improve the assessment's efficiency and accuracy. The interactions with MITRE may include technical consultation, supervised access to systems, , facilities, and monitoring assessment activities. Staff may be called upon on in ad-hoc manner via phone, email or in person conversations.

5.3 Onsite Schedule

The anticipated onsite schedule is for a **Kick-off meeting** to be held the morning of Monday August 19, 2013, and more detailed **walkthrough may follow**. Module testing will commence, with the scheduled completion on Friday August 30, 2013. No application interviews will be formally scheduled here. Ad-Hoc application interviews may be performed as needed and agreed upon by MITRE and CGI Federal. Joint daily outbriefs with the Data Service Hub, assessment running concurrently at QSSI in Columbia, MD, will be scheduled and documented elsewhere.

Day / Date	Time	Meeting
Mon 8/19	10:00 – 11:00	**Joint** Kick off Meeting
	11:00 - 11:30	FFM Eligibility & Enrollment (b)(5), (b)(6), (b)(7)c, (b)(7)e
	11:30 - Noon	FFM Eligibility & Enrollment My Account Demo
	Noon - 12:30	FFM & Hub Kickoff Meeting Lunch
	12:30 - 1:30	FFM E&E Individual Application Demo
	2:00 – 2:30	FFM E&E Direct Enrollment Demo
	2:30 – 3:30	**Joint** FTI Assessment Working Session
	3:30 – 4:30	FW: FFM DSH **Joint** SCA Daily Outbrief
Tue 8/20	3:30 – 4:30	**Joint** SCA Daily Outbrief
Wed 8/21	09:00-10:00	FFM Plan Management Demo
	3:30 – 4:00	**Joint** SCA Daily Outbrief
Thu 8/22	1:00 – 2:30	FFM Documentation Interview
	3:30 – 4:00	**Joint** SCA Daily Outbrief
Fri 8/23	3:30 – 4:00	**Joint** SCA Daily Outbrief
Mon 8/26	3:30 – 4:00	**Joint** SCA Daily Outbrief
Tue 8/27	1:00 – 2:30	FFM Application Developer Interview
	3:30 – 4:00	**Joint** SCA Daily Outbrief
Wed 8/28	9:30 – 11:00	FFM Database Administrator Interview
	3:30 – 4:00	**Joint** SCA Daily Outbrief
Thu 8/29	3:30 – 4:00	**Joint** SCA Daily Outbrief
Fri 8/30	3:30 – 4:30	**Joint** SCA Daily Outbrief

Note that where appropriate, the Business Owner or CMS ISSO is responsible for establishing interview appointments and teleconference bridges. The CMS Facilitator establishes DOB appointments and teleconference bridges.

5.4 Assessment Estimated Timeline

Table 137 describes the estimated timeline for assessment actions and milestones.

Table 137. Estimated Timeline for Assessment Actions and Milestones

Action/Milestone	Description	Date(s)
Provide scripts, data calls, or other	Lead evaluator provides the scripts, data calls	Monday July 22, 2013

Action/Milestone	Description	Date(s)
requests to CMS	or other requests for the Mainframe, Server O/S and Databases, when applicable	
Perform readiness review	Discuss assessment preparations and ensure tasks (e.g., account creation and providing documentation to MITRE) are on target for completion	Tuesday August 13,2013
Establish and test accounts	Set up and test all test accounts for the assessment	Monday August 12, 2013
Finalize and deliver Final Test Plan	Update the final test plan to include all action items, decisions, interview schedules, and other information from the Draft Test Plan Discussion	August 16, 2013
Deliver documentation, script output, and configuration output to MITRE	Deliver all documentation, script output, and configuration data to the MITRE Evaluation Team prior to onsite assessment	Monday August 12, 2013
Perform onsite assessment	Conduct technical testing and management and operations interviews based on the assessment's scope	August 19-30, 2013
Conduct final out brief	Review and summarize security vulnerabilities from assessment	Week of August 30, 2013
Last date to provide remediation evidence (if authorized by CMS Facilitator)	CMS Division of Information Security & Privacy Management strongly advices that the focus of remediation efforts be on addressing High risk findings, followed by Moderate risk findings. ***No application testing will be performed subsequent to the onsite.***	Friday September 6, 2013 (est.)
Remove security access	Remove security access established for MITRE test accounts	Friday September 6, 2013 (est.)
Deliver draft report to CMS	Put security vulnerabilities identified during the assessment into report format	Monday September 23, 2013
Review draft report	Answer questions and provide clarification. Only security vulnerabilities reported during the assessment and included in the final out brief are included in the report	Friday September 27, 2013
Deliver final report and data worksheet to CMS	Edit and clarify the draft report and generate a data worksheet	Friday October 4, 2013
Deliver final book package to CMS	Produce and provide hardcopies of test scripts, test data, out briefs, the final report, and the data worksheet(s) with a CD containing this information to the CMS SCAs GTL	Friday October 11, 2013