Office of Information Services
Division of Information Security & Privacy Management
Centers for Medicare & Medicaid Services

Federally Facilitated Marketplace (FFM) Security Control Assessment Test Plan

December 6, 2013

Final

Table of Contents

List of Tables

List of Figures

1. Introduction

1.1 Purpose

This document describes the security control assessment (SCA) methodology, schedule, and requirements that The MITRE Corporation (MITRE) will use to evaluate the Federally Facilitated Marketplace (FFM) application. The goal of the SCA Test Plan is to clearly explain 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 Control 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 a comprehensive scope SCA in accordance with the *CMS Information Security (IS) Certification & Accreditation (C&A) Program Procedures Version 2.1*[1] for the FFM application located at the (b)(5), (b)(6), (b)(7)c, (b)(7)e (b)(5), (b)(6), (b)(7)c, (b)(7)e The SCA complies with federal standards, policies, and procedures including the Federal Information Security Management Act of 2002 (FISMA), 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 Categorization of Federal Information and Information Systems*,[4] and then apply the appropriate

1 http://www.cms.gov/InformationSecurity/Downloads/CA_procedure.pdf (August 25, 2009).

2 http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf (August 2009).

3 http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf (March 2006).

4 http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf (February 2004).

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] *Business Partners Systems Security Manual Version 11.0 (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 upon 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 Blue Canopy's assessment methodology to verify and validate that the management, operational, and technical controls are appropriately implemented.

1.3.1 Phase 1: Planning

Phase 1, "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, "Assessment", 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 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

[5] http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/ARS.pdf (July 31, 2012).

[6] https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/PISP.pdf (August 31, 2010).

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

[8] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf (August 2013).

Team members. MITRE's evaluation goal is to apply experience and insight, in order to determine 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 application 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 FFM Application 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. 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

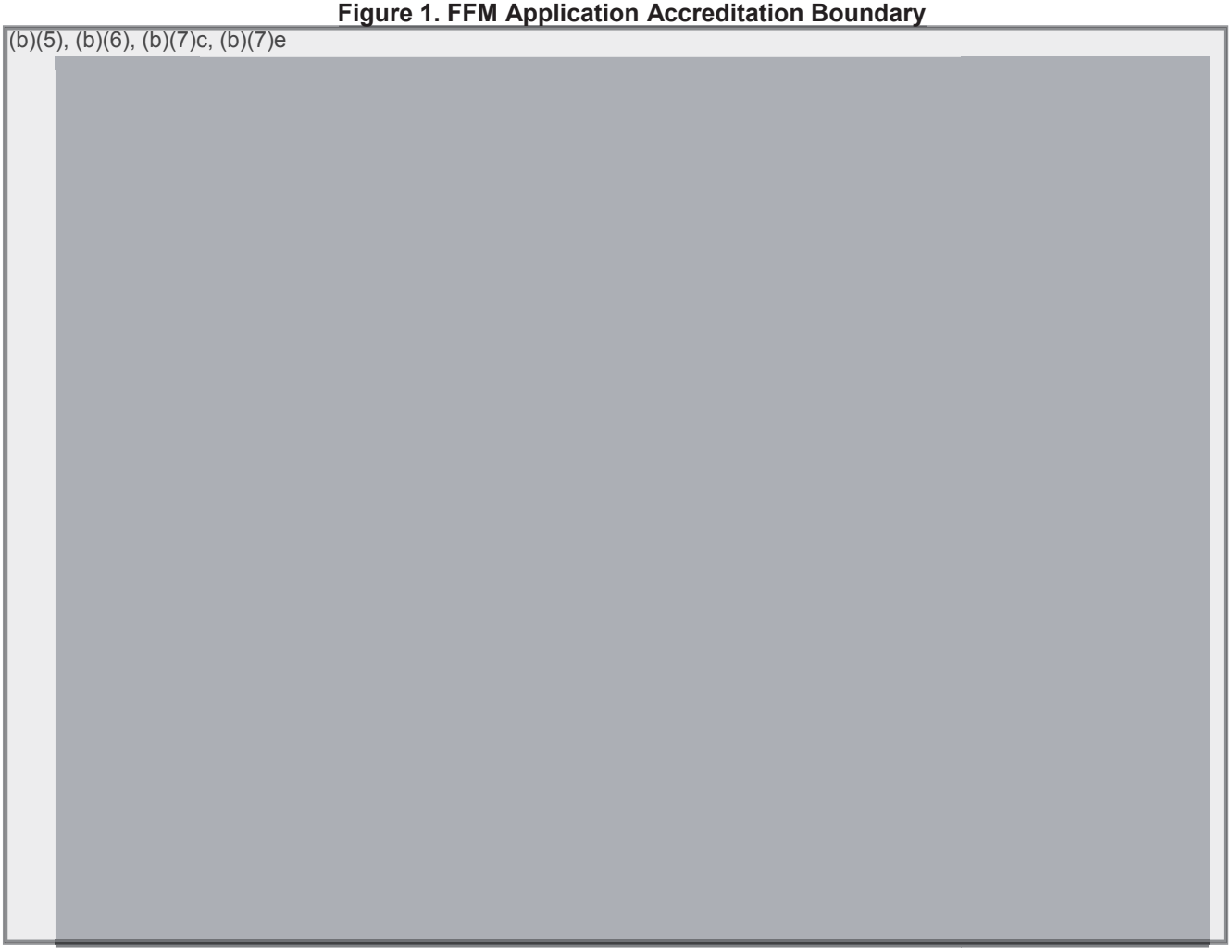
CCIIO will manage the Marketplace program and enable collaboration through 1) the use of a cloud-based infrastructure that is Federal Information Security Management Act (FISMA) compliant and can be dynamically scaled as needed, and 2) a secured cloud-based ALM that functions as a component of a Platform 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; and
- Delivery of a Health Insurance Plan structure for the States as many have requested such capabilities.

Figure 1 depicts the FFM application accreditation boundary.

Figure 1. FFM Application Accreditation Boundary



2.2 Assessment Scope

The goal of the SCA is to determine the extent to which the security controls, as defined in the CMS Minimum Security Requirements (CMSR) Acceptable Risk Safeguard (ARS), are present in the system and working as intended. There are certain limitations inherent in the methodologies implemented, and the assessment of security and vulnerability relating to information technology is an uncertain process based on past experiences, currently available information, and the anticipation of reasonable threats at the time of the assessment. There is no

assurance that an analysis of this nature will identify all vulnerabilities or propose exhaustive and operationally viable recommendations to mitigate all exposure.

MITRE is tasked with providing a Comprehensive Application Only SCA to determine if the FFM application has properly implemented CMS security standards. According to the System Security Plan (SSP), the FIPS 199 security categorization level for the FFM application is MODERATE due to the sensitivity of the information stored within the system (PII and sensitive documents from insurance companies). The SCA will examine the technical controls that support the FFM application to ensure adherence to the Moderate security level specifications in the CMS ARS CMSR, PISP, and BPSSM. Prior to the onsite, MITRE will make several requests for documentation and other related artifacts such as to adequately prepare for the onsite. To adequately perform the SCA.MITRE anticipates that the MITRE Evaluation Team will be onsite for ten days from December 9-20, 2013 at the CGI Federal offices located at 593 Herndon Parkway Herndon, Virginia.

MITRE will assess FFM R7.0.1.35/36(Build 294) in the (b)(5), (b)(6), (b)(7)c, (b)(7)c, (b)(7)e

The SCA scope will include the following:

- Application security testing of the FFM application including the following modules and functionalities:
  - *Eligibility and Enrollment (E&E):*
    - My Account
    - Individual Application
    - Plan Compare
    - Enrollment
    - Direct Enrollment
    - Eligibility Support Desktop (ESD)
    - Call Center Integration
  - *Plan Management (PM):*
    - Issuer Application Rate and Benefit Data Collection
    - Unified Rate Review
    - Cross Validation
    - State Evaluation
    - Plan Transfer (SERFF/OPM)
    - Plan Certification
    - Plan review
  - *Financial Management (FM):* (b)(5), (b)(6), (b)(7)c, (b)(7)e
  - *Plan Data Validator:* (b)(5), (b)(6), (b)(7)c, (b)(7)e authentication mechanisms to FFM)
  - *Reporting/Data Warehouse* (b)(5), (b)(7)c, (b)(7)e and authentication mechanisms to FFM)

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

- Interviews will be conducted with database and application technical resources

CMS, CGI and MITRE determined that the following functionalities and activities **will not** be in the scope:

- FFM Application Functionalities/Modules:
  - *Eligibility and Enrollment (E&E):*
    - Notices & Mailing – functionality not currently active in production
  - *Plan Management (PM):*
    - Deficiency Notices – functionality not currently active in production
  - *Financial management:*
    - SBM Data Collection – functionality not currently active in production
    - CSR Calculation – functionality not currently active in production
  - *Customer Service:*
    - Entire module – functionality not yet developed
  - *Quality:*
    - Entire module – functionality not currently active in production
  - *Oversight:*
    - Entire module – functionality not currently active in production
- System Level Components (hardware, operating systems, etc.)

  This is a comprehensive application only assessment - all system-level/General Support System related components are out of scope.
- ARS 1.5 Management and Operational Controls

  Management and Operational controls Operations such as Configuration Management, Contingency Planning, Incident Response, etc. will not be tested during this SCA. CMS stated that previous assessments of these controls were sufficient.
- Written evaluations of the System Security Plan, Information Security Risk Assessment and Contingency Plan documents will not be performed.

MITRE will also determine if FFM application management and support personnel have an understanding of the CMS Information Security (IS) ARS including CMSR Version 1.5, *HHS Minimum Security Configuration Standards for Departmental Operating Systems and Applications*[9], CMS PISP, and BPSSM, as appropriate.

[9] http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/is_baseline_configs.pdf (May 3, 2012).

Application testing will be performed in (b)(5), (b)(6), (b)(7)c, (b)(7)e environment, and in adherence to the *CMS Information Security (IS) Assessment Procedure Version 2.0*[10] 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 technical security control families will be the focus for testing:

- Access Control (AC), all controls except AC-1, AC-18, AC-19, AC-20(2)
- Audit and Accountability (AU), all controls except AU-1
- Configuration Management (CM), CM-3 and CM-8 only
- Identification and Authentication (IA), all controls except IA-1
- System Communications (SC), all controls except SC-1, SC-4, SC-18, SC-20, SC-21, SC-22
- System and Information Integrity (SI), all controls except SI-1, SI-3, SI-5, SI-8

2.3 Assessment Assumptions/Limitations

Assumptions

- Operating Systems images (b)(5), (b)(6), (b)(7)c, (b)(7)e (Routers, Switches, etc.) are out of scope.
- Akamai, GovDelivery Transactional Messaging Service (TMS) and Assets Framework and all their services are out of scope.
- Previous assessments of FFM's Management and Operational controls are sufficient. Additional activities for the specific review of these controls will not be included in the scope of this assessment.
- The (b)(5), (b)(6), (b)(7)c, (b)(7)e be free of performance and stability issues that could adversely affect the application security testing activities.
- No code changes, hot fixes, etc. deployed to the SCA testing environment during the two week SCA onsite visit unless otherwise approved by MITRE.
- The application under test shall be completely free of defects or incomplete code that would prevent the application security tester from proceeding through the application in a manner consistent with an actual user experience.
- All FFM modules and functionality shall be available for testing within a single environment.
- MITRE Evaluation Team personnel will have unrestricted access to (b)(5), (b)(6), (b)(7)c, (b)(7)e environment between the hours of 9:00am and 6:00pm and to all required components within the scope of the assessment
- Information system accounts will be provisioned and tested prior to the first day of onsite testing.
- Appropriate data will be pre-populated into the system as discussed during the December 2, 2013 Application Workflow meeting.

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

- CMS and CGI Federal POCs will be available for support during the SCA onsite visit.
- All persons involved in the interview process will be available during their designated interview times.
- The CMS and CGI Federal POCs will provide the SCA Team with accurate information and evidence at all times.
- 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.
- The MITRE Evaluation Team will have access to all relevant documentation for the system.
- Information requested by MITRE will be delivered in a timely manner.
- All GSS policies and procedures that govern the testable modules are the same policies and procedures that were assessed as part of the HIX/QHP assessment March-April 2013.
- Assessment of remediation evidence for findings documented in previous SCAs is considered to be secondary activity and will be performed only if time and resources permit.
- Test accounts will be made available for every role within the application, prior to the onsite date.
- Some test accounts will be configured to allow testers to assess beginning at key points within the application/workflow process.
- 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 Blue Canopy 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 Blue Canopy 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 is 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 Blue Canopy 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 SCA 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 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.

2.5.6 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, must be a CMS employee, and can be a System Developer/System Maintainer ISSO.

2.5.7 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 SCA Report (e.g., Findings Report) to communicate how the CMS business mission will be impacted if an identified vulnerability is exploited.

2.5.8 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 Assessment Responsibility Assignment

For this assessment, MITRE, CMS, and CGI Federal staff names have been associated with their 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
Jessica Hoffman Jason King Jane Kim	CMS/OIS CMS/OIS CMS/OIS	CMS Facilitator (Lead) CMS Facilitator (Backup) CMS Facilitator (Backup)
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
Milton Shomo	MITRE	SCA Project Lead
Jim Bielski	MITRE	SCA Deputy Project Lead/ Application Assessor
Tom Kirk	CGI Federal	Program Manager
Hemant Sharma	CGI Federal	Architecture Teams Manager
Ned Hammond	CGI Federal	Production Operations Manager
Rich Bissonette	CGI Federal	Application Management Manager
Candice Ling	CGI Federal	Business Operations Manager
Balaji Ramamoorthy	CGI Federal	Senior Security Architect
Raj Sundar	CGI Federal	Security Architect
Joel Singer	CGI Federal	Deployment Manager
Patrick Cronin	CGI Federal	Monitoring & Reporting Manager

Name	Organization	Role
Danny Dohnalek	CGI Federal	Environment Manager
Taulant Shamo	CGI Federal	Operations Manager
Monica Winthrop	CGI Federal	Release Management Manager
Bob Neidecker	CGI Federal	Application Maintenance Manager

2.7 Physical Access and Work Area Requirements

The MITRE Evaluation Team will require direct network connectivity to the FFM application in (b)(5), (b)(6), (b)(7)c, (b)(7)e also network access to the Internet. A work area needs to be established, and should include; power, outside internet, table, and chairs. In addition, the MITRE Evaluation Team will require a separate work area for conducting interviews and analyzing data.

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)

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 requested documentation and artifacts in a timely manner to avoid delays and improperly reporting findings. In order to effectively perform the assessment and have no delays in the SCA, the MITRE Evaluation Team 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, and potentially reporting false findings. ***To assist MITRE in determining the completeness of this information and to serve as a checklist, CMS, and CGI Federal should use Table 2 through*** **Error! Reference source not found.** ***as a prioritized request list, and include any comments that may be applicable (e.g., System Design Document [SSD] contains detailed network diagram, SSP contains hardware and software inventory, and configuration management document contains baseline configurations and approved exceptions to baselines).***

Tier 1 Documentation - Mandatory Pre-Assessment: These documents are extremely helpful in determining the system accreditation boundary, devices in scope, number of components and complexity, etc. Draft versions of the documents listed in Table 2 were provided the week of November 11, 2013 for use in the development of the draft test plan.

Table 2. Tier 1 Documentation – Mandatory Pre-Assessment

Document Element #	Document/Information Requested	ARS CMSR	Comments
D01	Information System Risk Assessment (ISRA)	RA-3 Risk Assessment	Final pending
D02	System Security Plan (SSP) • SSP Workbook • SSP approval / certification evidence	PL-2 System Security Plan CA-4 Security Certification	Final received 11/25/2013
D03	Contingency Plan. This includes: • Facility and telecommunications failover • Fail-back planning • CP approval / certification evidence	CP-2 Contingency Plan	Final received 11/25/2013
D04	Detailed network diagram including IP addresses of devices	CM-2 Baseline Configuration	Received 11/12/2013
D05	Hardware and software inventories	CM-2 Baseline Configuration CM-8 Information System Component Inventory	Received 11/12/2013

Tier 2 Documentation: MITRE uses the time prior to the onsite to review documentation, system baseline configurations, or process evidence to prepare for deep-dive analysis into processes, procedures, or technical settings. To facilitate this, the documents in Table 3 must be provided a week prior to the onsite. This will allow MITRE time to identify gaps in the documentation, such as references to supplemental documentation residing on SharePoint/network folders which was not originally provided. If the provided documentation does not fully meet the information request, MITRE will identify such gaps to CMS and CGI Federal staff, so they can quickly retrieve and provide the additional information.

Table 3. Tier 2 Documentation - Required Two Weeks Prior to Onsite

Document Element #	Document/Information Requested	ARS CMSR	Comments
D06	List of ***open*** Plan of Action and Milestones (POA&M) within the CMS FISMA Control Tracking System (CFACTS)	CA-5 Plan of Action and Milestones (POA&M)	

Document Element #	Document/Information Requested	ARS CMSR	Comments
D07	Provide documentation describing UserID conventions such as: • Account naming conventions, defined groups (Administrator, User, Contractor, etc.), and conditions for group membership • Processes and tools used for monitoring adherence to CMS ARS account management and password directives	AC-2 Account Management IA-4 Identifier Management IA-5 Authenticator Management	
D08	Provide evidence that reflects information system accounts and group membership are reviewed and certified, per CMS ARS directives.	AC-2 Account Management	
D09	Documentation describing the types of audit logging that is implemented for FFM in support of CMS policies.	AU-2 Auditable Events AU-3 Content of Audit Records AU-12 Audit Generation	
D10	Process/procedure documentation that describes how audit records are securely stored/protected and ensures no loss of data due to processing failures • Should describe the specific technologies utilized to either prevent or alert staff when a failure occurs or is pending (due to storage issues etc.)	AU-4 Audit Storage Capacity AU-5 Response to Audit Processing Failures	

Document Element #	Document/Information Requested	ARS CMSR	Comments
D11	Process/procedure documentation that describes how audit information is protected from unauthorized access (read and update) and non-repudiation mechanisms • Should describe both the tool protections specifically employed as well as non-tool access (e.g., if a database/data store is used, how is this data protected from direct access for read/update) • Should describe which information system components have implemented non-repudiation services and the associated actions under protection; description should explain the technologies used to deploy the non-repudiation service	AU-9 Protection of Audit Information AU-10 Non-Repudiation	

3.1.3 Script Output Requirements

MITRE must obtain (b)(5), (b)(6), (b)(7)c, (b)(7)e ***output and completed*** (b)(5), (b)(6), (b)(7)c, (b)(7)e ***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 FFM application, accounts that reflect the different user types and roles need to be created and tested prior to the MITRE Evaluation Team 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.***

Testing will be performed in the (b)(5), (b)(6), (b)(7)c, (b)(7)e testing environment. Based on the defined assessment scope, the application roles and responsibilities/privileges are listed in **Error! Reference source not found.** and **Error! Reference source not found.**.

Table 4. Eligibility and Enrollment User Roles

Role	Description
Agent/Broker	An Agent/Broker will have access to the agent or broker's personal portal, which contains profile and license information. The Agent/Broker will also have access to the accounts of any employers, employees, or individuals with whom the agent or broker has an agreement. The Agent/Broker will have access to all data in the FFM corresponding to a client's account and will be able to update the client's account.
Application Filer	The Application Filer will have access to all data in FFM corresponding to the filer's account. The Application Filer will have the ability to start/continue an application, enroll in a plan, upload additional documentation, and edit account information.
Authorized Representative	The Authorized Representative will have access to all data in FFM corresponding to the accounts with which they are associated. The access level for the Authorized Representative will be defined by the Application Filer or an associated individual.
Customer Care Representatives	Customer Care Representatives (CCR) have access to data in the Marketplace relevant to an individual to assist individual in applying for health insurance coverage. These users have view and edit privileges for data in the Marketplace. This user role will be elaborated upon in future releases.

Table 5. Plan Management User Roles

Role	Description
QHPSubmitter (Issuer Module)	An individual who is assigned the user access role of data submitter will submit the data necessary to complete the Issuer Module. They will also have the ability to cross validate Final Submission data elements to ensure they are consistent throughout an application.
QHPValidator (Issuer Module)	An individual who is assigned the user access role of data validator will validate all sections of the Issuer Module for accuracy. They will also have the ability to cross validate that Final Submission data elements are consistent throughout an application, and "Submit" the application after successful cross validation.
BenefitsSubmitter (Benefits and Service Area Module)	An individual who is assigned the user access role of BenefitsSubmitter will submit the data necessary to complete the Benefits and Service Area module. They will also have the ability to cross validate Final Submission data elements to ensure they are consistent throughout an application.

Role	Description
BenefitsValidator (Benefits and Service Area Module)	An individual who is assigned the user access role of BenefitsValidator will be responsible for validating the data necessary to complete the Benefits and Service Area module. They will also have the ability to cross validate that Final Submission data elements are consistent throughout an application, and "Submit" the application after successful cross validation.
RatingSubmitter (Rating Module)	An individual who is assigned the user access role of data submitter will submit the data necessary to complete the Rating Module. They will also have the ability to cross validate Final Submission data elements to ensure they are consistent throughout an application.
RatingValidator (Rating Module)	An individual who is assigned the user access role of data validator will validate all sections of the Rating Module for accuracy. They will also have the ability to cross validate that Final Submission data elements are consistent throughout an application, and "Submit" the application after successful cross validation.
UnifiedRateReviewIssuerSubmitter (Rate Review Module)	An individual who is assigned the user access role of the UnifiedRateReviewIssuerSubmitter creates Rate Filing Justification submissions to either be filed or rate reviewed. This user has access to all functions of the application for submitting submissions. Access to data is determined through the associated Issuer account X-Reference in HIOS.
UnifiedRateReviewIssuerValidator (Rate Review Module)	An individual who is assigned the user access role of UnifiedRateReviewIssuerValidator attests to the validity of the submission's created by Issuer-Submitters before a rate review takes place. This user has access to all functions of the application for validating submissions. Access to data is determined through the associated Issuer account X-Reference in HIOS.
UnifiedRateReviewState (Rate Review Module)	An individual who is assigned the user access role of UnifiedRateReviewIssuerValidator attests to the validity of the submission's created by Issuer-Submitters before a rate review takes place. This user has access to all functions of the application for validating submissions. Access to data is determined through the associated Issuer account X-Reference in HIOS.
UnifiedRateReviewContentReviewer (Post Launch) (Rate Review Module)	An individual who is assigned the user access role of UnifiedRateReviewContentReviewer (Post Launch) ensures a content review on submissions that ensures that submitted materials are suitable for posting on government health care websites. This user has access to functions of the application that pertain to conducting content assessment of submissions and assigning of Contractors to a submission.
UnifiedRateReviewContractor (Rate Review Module)	An individual who is assigned the user access role of UnifiedRateReviewContractor is assigned to CMS Primary submissions to submit reports to help CMS Reviewers conduct rate reviews. This user has access to all functions of the application for reviewing and uploading reports to provide detailed information on submissions. Access to data is determined through the associated Contractor account X-Reference in HIOS and designation within the submission by a CMS user.

Role	Description
UnifiedRateReviewCMS (Rate Review Module)	An individual who is assigned the user access role of UnifiedRateReviewCMS conducts rate reviews on submissions that are deemed CMS Primary.This user has access to all functions of the application for reviewing and providing a determination for submission identified as CMS Primary
UnifiedRateReviewAdministrator (Rate Review Module)	An individual who is assigned the user access role of UnifiedRateReviewAdministrator performs all Issuer and Reviewer functionality in the system, in addition to setting the rules that determine if a submission should be State or CMS Primary in each state. This user has access to all functions of the application for all other user types. This user additionally has the unique ability to deem submission suitable for Web Posting on HealthCare.gov, as well as assign a state's primary type.
CategoryClassCountUser (USP Category Class Count Service Module)	An individual who is assigned the user access role of CategoryClassCountUser will have the ability to upload a list of RxCUI's into the Service and receive any of the resulting reports.
QHP, Benefits and Rating Submitters (Final Submission Module)	Individuals who are assigned the user access roles of data submitters will cross validate the submitted and/or validated data from the Issuer, Benefits, Rating and Rate Review Module. They will have the ability to cross validate Final Submission data elements to ensure they are consistent throughout an application.
QHP, Benefits and Rating Validators (Final Submission Module)	Individuals who are assigned the user access roles of data validators will cross validate submitted and/or validated Final Submission data elements from the Issuer, Benefits, Rating and Rate Review Module for accuracy. They will also have the ability to "Submit" the application after successful cross validation.
QHPStateReviewer (QHP State Evaluation Module)	An individual who is assigned the user access role of QHPstatereviewer has access to the State Evaluation module and view access to the Issuers in their State.
QHPCMSReviewer (CMS Certification Module)	An individual who is assigned the user access role of QHPcmsreviewer will have access to the CMS Certification module and the ability to suppress plans.

(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 its security policies.

3.2.1 Documentation Review

Prior to, and during the assessment, the MITRE Evaluation Team will review documents provided by CMS and CGI Federal. The information obtained from this review will be used to augment technical controls testing. For example, if the ARS CMSR stipulates that the password length for the information system is required to be eight characters, and the SSP documents that the length of passwords is eight characters, the technical assessment will confirm whether passwords are configured to be eight characters in length. In general, the MITRE Evaluation Team will review, but not be limited to, the following sample set of documentation: SSP, ISRA, and CP. For the complete documentation list, refer to Section 3.1.2.

3.2.2 Vulnerability Assessment Tools

MITRE will work with CMS and CGI 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:

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

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

The list above is not all inclusive. MITRE will use other tools and scripts, as needed, and provide test scripts to CMS to share with necessary support staff. As much as possible, MITRE will avoid affecting out-of-bounds systems; however, tools may send non-standard network traffic, which could affect non-targeted (out-of-bounds) hosts if located on the same network. The effects of network-based tools will be contained within the in-bound portions of the target environment to the greatest extent possible.

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:

- Collect artifacts/evidence that demonstrate the CMS security controls are operating as required
- Conduct security control testing with full knowledge of the system, applications, products, configurations, and topology
- Provide MITRE Evaluation Team members, who have specific knowledge of; Web systems, and Web programming technologies (b)(5), (b)(6), (b)(7)c, (b)(7)e (b)(5), (b)(6), (b)(7)c, (b)(7)e and database technologies
- Attempt to gain unauthorized user access or unauthorized access to system resources and data
- Determine the system's susceptibility to (b)(5), (b)(6), (b)(7)c, (b)(7)e
- Identify system vulnerabilities based on the following items:
  - Architecture design and implementation
  - Published or known weaknesses, bugs, advisories, and security alerts about the 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
  - Evaluation of Web application buffer overflow and password vulnerabilities by performing tests that include brute force password attacks and buffer overflow
- Observe personnel, physical, and other security controls while onsite and during the course of the assessment
- Examine database configuration settings

3.3.1 Interviews

Interviews will focus on a review of the 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.

3.3.2 Application Testing

The MITRE Evaluation Team will test the FFM application to ensure proper software development techniques, supported software is used, and that the Confidentiality, Integrity and Availability (CIA) of data processed by the application adheres 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

CMS or 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. Where possible, at least one account should have administrative access with the ability to adjust the application roles of another account.

3.3.3 Database Instance Testing

The MITRE Evaluation Team will evaluate database 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 the results of MITRE assessment test scripts to identify known flaws in the (b)(5), (b)(6), (b)(7)c, (b)(7)e versions and settings
- Review database security configuration settings to determine if adequate system protections are implemented
- Interview the database administrators (if required) concerning database system configurations and security relevant mechanisms

4. Reporting

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

4.1 Security Control Assessment Findings Spreadsheet

The SCA findings spreadsheet (Table 6) is a running tabulation of findings identified during the assessment that is reviewed during Daily Out-Briefs (DOBs). 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.

Table 6. Findings Spreadsheet

n 1 and GSS Assessment

Weakness	Risk Level	CMSR Security Control Family	Reference	Affected Systems	Ease-of-Fix	Est Work Effort	Finding	Failed Test Description	Actual Test Results	Recommended Corrective Actions	Status
Wednesday September 1, 2010											
CMS zoned architecture not properly implemented	Moderate	Access Control (AC)	AC-4	GSS	Moderately Difficult	Substantial	The CMS multi-zone architecture as defined in the CMS Technical Reference Architecture (TRA) has not been properly implemented. A single Cisco ASA firewall is used to separate the presentation and application zones instead of individual separate redundant firewalls at each zone. A pair of redundant Cisco switches with VLANs provide connectivity to these zones instead of dedicated redundant switches at each zone. The Management Zone is incorporated into the production zones and not a separate zone. Since a single firewall is protecting both the presentation and application zones, the security risk is a breach of the firewall could result in a Denial of Service, exposure of PII or PHI or corruption of sensitive data.	The CMS Technical Reference Architecture (TRA), and its associated Supplements, documents the standard architecture for all of the CMS Production environments. The Supplements document specific technical solutions in support of the TRA. The current TRA and relevant published Supplements are listed below: CMS Technical Reference Architecture, ver 2.0, November 2009 - Security Services, ver 1.0, November 2009	A single Cisco ASA firewall is used to separate the application and data zones instead of individual separate redundant firewalls at each zone. A pair of redundant Cisco switches with VLANs provide connectivity to these zones instead of dedicated redundant switches at each zone. The Management Zone is incorporated into the production zones and not a separate zone.	Implement separate physical firewalls between the presentation, application, data, and management network zones that support filtering based on source/destination address and ports as well as protocol and service. Firewalls should support stateful and deep packet inspection at the IP, protocol, and application layer. Firewalls must be from different vendors between tiers. Implement dedicated redundant switches within each tier. Establish an isolated Management Zone and relocate all management functions and traffic to this zone. Production resources that require SMTP, FTP, POP or other core services should be utilizing those services hosted in the Management Zone and not communicate directly with the Internet. See TRA Section 2.3 Management Zone for more information.	Identified September 1, 2010.
Web application does not restrict storage of passwords	Moderate	Identification and Authentication (IA)	IA-2	Application Name	Easy	Minimal	The Web application allows users to save their user ID and password within the Web browser such that they are not required to manually enter them during subsequent connections. This presents the opportunity for unauthorized access to the application if an attacker obtains authentication information from the browser cache.	The CMSR requires the use of [illegible] authenticators and unique user ide[illegible]	Users a[illegible] connect to the application without being prompted [illegible]	Configure the application to require the users to manually enter their credentials prior to each session. Disable the AUTOCOMPLETE attribute in any HTML forms or individual input elements containing passwords. For example, AUTOCOMPLETE="OFF".	Identified September 1, 2010. On Se[illegible] the contractor provided evidence of remediation. MITRE reviewed this and closed this finding.
Browser caching of secure pages not restricted	Moderate	System and Communications Protection (SC)	SC-4	Application Name	Easy	Minimal	The Web application allows secure pages to be stored in the local browser cache. The security risk is the cache can be subsequently accessed to retrieve sensitive information.	[illegible] CMSR, controls [illegible] produced [illegible] users [illegible] acting on behalf of a [illegible] current user (procured [illegible] access to a shared system [illegible] released back to the information [illegible]. There shall be no residual information from the [illegible]	The Web application allows secure pages to be stored in the local browser cache.	Configure the application to prevent browser caching. Set HTTP headers to "Pragma: No-cache" and "Cache-control: No-store". Alternatively, this can be set in the HTML header to: <META HTTP-EQUIV="Pragma" CONTENT="no-cache"> and <META HTTP-EQUIV="Cache-Control" CONTENT="no-store">, but some browsers may have problems using this method.	Identified September 1, 2010.
Audit settings do not conform to CMS guidelines	Moderate	Audit and Accountability (AU)	AU-2	Server 1, Server 2, Server 3	Easy	Minimal	[illegible] audit [illegible] CMS [illegible] successful events. The security [illegible] could go undetected.	Per the CMSR, automated mechanisms shall be established which enable the ability to generate an audit record for a pre-defined set of events that are adequate to support after-the-fact investigations of security incidents. The selection of auditable events shall be based upon a risk assessment as to which events require auditing on a continuous basis, and which events require auditing in response to specific situations.	Auditing is set to only record successful events.	Change the Windows audit settings to the following: Account Logon = Success, Failure; Account Management = Success, Failure; Directory Service Access = No auditing (except for domain controllers, then failure only); Logon = Success, Failure; Object Access = Failure (may cause excessive logentries); Policy Change = Success, Failure; Privilege Use = Failure; Process Tracking = No auditing; System = Success, Failure	Identified September 1, 2010.
Verbose error messages	Low	System and Information Integrity (SI)	SI-11	Application Name	Moderately Difficult	Moderate	When an error is triggered in the application, a stack trace is presented to the user. A malicious user could use this information to craft an exploit or as verification of a successful exploit. A malicious actor could potentially use the verbose information to craft an attack within the application to gain unauthorized access to the application or CMS data.	Per the CMSR, information systems are to employ automated mechanisms that generate error messages providing timely and useful information to users without revealing information that could be exploited by adversaries.	MITRE attempted to connect to the following URLs: https://sample.url.org/... and https://sample2.url.org	Configure the application to catch all errors and provide the user with a generic error message that lacks any detailed information.	Identified September 1, 2010.

4.1.1 Row Number

Each vulnerability 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's current implementation of the underlying technology and the assessment guidelines contained with the *CMS Reporting Procedure for Information System (IS) Assessments* document,[11] MITRE will assign these values to each Business Risk. The risk ratings are described in Table 7.

Table 7. Risk Definitions

Rating	Definition of Risk Rating
High Risk	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 Risk	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 Risk	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
Observations	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)

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

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.), which are 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 8.

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 9.

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

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 weeks, 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 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 ulnerabilities 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.

4.4 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 or ISSO.

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 provided such evidence is received by MITRE within 5 business days of the final out-brief. 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 requires 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 draft test report. Following a draft test report review conference call that will be scheduled by CMS, MITTRE 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 SCA Evaluation Team POCs for the SCA are listed in Table 10.

Table 10. SCA Evaluation Team Points of Contact

Name	Position	Phone Number	Email Address
Milton Shomo	SCA Project Lead	(571) 329-8451	tshomo@mitre.org
Jim Bielski	Application Tester	(410) 902-2717	jbielski@mitre.org
Hoa Duc Do	Application Tester	(703) 983-6052	hoado@mitre.org
Jose Cintron	Application Tester	(703) 983-3040	jcintron@mitre.org
Jonathan Jones	Application Tester	(703) 343-6413	jonesj@mitre.org
Chriss Koch	Application Tester	(719) 572-8223	cgk@mitre.org
Farzan Karimi	Application Tester – Blue Canopy	(570) 885-6325	fkarimi@bluecanopy.com
Jason Pelker	Application Tester – Blue Canopy	(571) 218-8835	jpelker@bluecanopy.com
Harvey Rubinovitz	Database Assessor	(781) 271-3076	hhr@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 11.

Table 11. CMS Points of Contact

Name	Position	Phone Number	Email Address
Jessica Hoffman	CMS/OIS Facilitator	(410) 786-4458	jessica.hoffman@cms.hhs.gov
Jason King	CMS/OIS Facilitator	(410) 786-7578	jason.king@cms.hhs.gov
Tom Schankweiler	CMS/ISSO	(410) 786-5956	thomas.schankweiler@cms.hhs.gov
Darrin Lyles	CMS/ISSO	(410) 786-4744	darrin.lyles@cms.hhs.gov
Kirk Grothe	CMS Maintainer	(301) 492-4377	kirk.grothe@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 12.

Table 12. Vendor Points of Contact

Name	Position	Phone Number	Email Address
Lynn Goodrich	FFM Assessment POC and Lead Security Analyst	(301) 706-9776	lynn.goodrich@cgifederal.com
Greg Caulfield	FFM Secondary Assessment POC and Security Analyst	(908) 400-1935	greg.caulfield@cgifederal.com
Balaji Ramamoorthy	FFM Lead Security Architect and Primary Technical POC	(518) 461-9590	balajimanikandan.ramamoorthy@cgifederal.com
Raj Sundar	FFM Security Architect and Secondary Technical POC	(732) 675-9322	raj.sundar@cgifederal.com
Tom Kirk	FFM Program Manager	(703) 851-0092	thomas.kirk@cgifederal.com
Candice Ling	FFM Business Operations Manager	(703) 227-6320	candice.ling@cgifederal.com
Rich Bissonette	FFM Application Management Manager	(703) 227-5543	richard.bissonette@cgifederal.com
Joel Singer	FFM Deployment Manager	(703) 272-9522	joel.singer@cgifederal.com
Hemant Sharma	FFM Architecture Teams Manager	(703) 227-4588	hemant.sharma@cgifederal.com
Ned Hammond	FFM Production Operations Manager	(703) 267-8342	ned.hammond@cgi.com
Patrick Cronin	FFM Monitoring & Reporting Manager	(703) 227-6934	patrick.cronin@cgifederal.com
Danny Dohnalek	FFM Environment Manager	(703) 227-4257	daniel.dohnalek@cgi.com
Taulant Shamo	FFM Operations Manager	(703) 251-5110	taulant.shamo@cgifederal.com
Monica Winthrop	FFM Deputy Project Manager	(703) 227-6012	monica.winthrop@cgifederal.com
Bob Neidecker	FFM Application Maintenance Manager	(703) 227-5590	bob.neidecker@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, networks, infrastructures, facilities, and monitoring assessment activities. The following calendar outlines anticipated staff requirements.

The anticipated staff requirements can be found in Table 13 and 14.

All positions are expected to attend, or be available for, the daily out-briefs.

Table 13. Anticipated Staff Requirements for the week of 12/9/2013

Position	Day 1: Dec 9	Day 2: Dec 10	Day 3: Dec 11	Day 4: Dec 12	Day 5: Dec 13
Application Developer/Administrator	KO/A	A	A	A	A
Database Administrator(s)	KO/A	A	A	A	A
Program Manager/Business Owner/ System Owner	KO	A	A	A	A

Legend: I = Interview; KO = Kick-off Meeting; A = Available (On-Call), T = Tour

Table 14 - Anticipated Staff Requirements for the week of 12/16/2013

Position	Day 6: Dec 16	Day 7: Dec 17	Day 8: Dec 18	Day 9: Dec 19	Day 10: Dec 20
Application Developer/Administrator	A/I	A	A	A	A
Database Administrator(s)	A	A	A	A/I	A
Program Manager/Business Owner/ System Owner	A	A	A	A	A

Legend: I = Interview; KO = Kick-off Meeting; A = Available (On-Call), T = Tour

5.3 Onsite Schedule

MITRE's onsite schedule can be found in Table 15 and 16. All times listed are Eastern Standard Time (EST).

Table 15. MITRE Evaluation Team Onsite Schedule for the week of December 9, 2013

Day 1: December 9	Day 2: December 10	Day 3: December 11	Day 4: December 12	Day 5: December 13
Arrive onsite at 8:30.am. (Local)	Arrive onsite at 8:30a.m. (Local)	Arrive onsite at 8:30a.m. (Local)	Arrive onsite at 8:30a.m. (Local)	Arrive onsite at 8:30a.m. (Local)
Set up work space and establish procedures for network connection (Section 3.1)	Perform application testing	Perform application testing	Perform application testing	Perform application testing
Conduct "Kick-off" meeting, review relevant documents (diagrams, workflows etc.) and perform application walk through 9:00am – 12:00pm				
Perform application testing	Perform application testing	Perform application testing	Perform application testing	Perform application testing
	Prepare for DOB	Prepare for DOB	Prepare for DOB	Prepare for DOB
	Conduct DOB at 3:30p.m.	Conduct DOB at 3:30p.m.	Conduct DOB at 3:30p.m.	Conduct DOB at 3:30p.m.

Table 16. MITRE Evaluation Team Onsite Schedule for the week of December 9, 2013

Day 10: December 16	Day 11: December 17	Day 12: December 18	Day 13: December 19	Day 14: December 20
Arrive onsite at 8:30a.m. (Local)	Arrive onsite at 8:30a.m. (Local)	Arrive onsite at 8:30a.m. (Local)	Arrive onsite at 8:30a.m. (Local)	Arrive onsite at 8:30a.m. (Local)
Perform application testing	Perform application testing	Perform application testing	Perform application testing	Conclude application testing
Application Developer Interview (1.5 hours): Interview the Application Developers to assess AC, AU, CM, and MA security controls 9:30am – 11:00am			Examine implementation and configuration of databases	
Perform application testing				
Examine implementation and configuration of databases	Examine implementation and configuration of databases	Examine implementation and configuration of databases	**Database Admin Interview (1.5 hours):** Interview the DBAs to review and assess the implementation and configuration of databases, account management processes, auditing, maintenance procedure, etc. 1:00pm – 2:30pm	
Prepare for DOB	Prepare for DOB	Prepare for DOB	Prepare for DOB	
Conduct DOB at 3:30p.m.	Conduct DOB at 3:30p.m.	Conduct DOB at 3:30p.m.	Conduct DOB at 3:30p.m.	

Note that where appropriate, the Business Owner or CMS Facilitator will be responsible for establishing teleconference bridges.

5.4 Assessment Estimated Timeline

Table 17 describes the estimated timeline for assessment actions and milestones.

Table 17. Estimated Timeline for Assessment Actions and Milestones

Action/Milestone	Description	Date(s)
Status Meeting	Discuss open action items and updates to the assessment.	11/25/2013
Perform Readiness Review	Discuss assessment preparations and ensure tasks (e.g., account creation and providing documentation to Blue Canopy) are on target for completion	12/2/2013
Establish and test accounts	Set up and test all test accounts for the assessment	12/2/2013
Deliver documentation, script output, and configuration output to Blue Canopy	Deliver all documentation, script output, and configuration data to the Blue Canopy Evaluation Team prior to onsite assessment	12/2/2013
Functionality list	CGI will provide a list of inoperable and/or undeveloped functionalities within the FFM application where assessors may encounter errors.	12/2/2013
Perform Onsite Assessment	Conduct technical testing and management and operations interviews based on the assessment's scope	12/9/2013 – 12/20/2013
Conduct Final Out-Brief	Review and summarize security vulnerabilities from assessment	1/7/2014
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	1/13/2014
Remove security access	Remove security access established for Blue Canopy test accounts	1/6/2014
Deliver Draft SCA Report to CMS	Put security vulnerabilities identified during the assessment into report format	1/28/2014
Review Draft SCA 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	Within 5 business days of deliver of the draft report
Deliver Final SCA Report and CFACTS Worksheet to CMS	Edit and clarify the Draft SCA Report and generate a CFACTS Worksheet	2/7/2014
Deliver Final SCA 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	2/13/2014

CENTERS FOR MEDICARE & MEDICAID SERVICES

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

Federal Data Services Hub (DSH) Security Controls Assessment Test Plan

August 20, 2013

FINAL

Table of Contents

List of Tables

List of Figures

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 theData Service Hub (DSH) major application. 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 Quality Software Services, Inc (QSSI) technical managers, 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 a comprehensive scope SCA in accordance with the *CMS Information Security (IS) Authorization To Operate Package Guide, v2.0*[1] forDSH Major Application housed at the (b)(5), (b)(6), (b)(7)c, (b)(7)e
The 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 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.

---

[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.

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

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] *Business Partners Systems Security Manual Version 10.0 (BPSSM)*,[7] and *CMS Technical Reference Architecture (TRA) Version 2.1*.[8] 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*[9] 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 QSSI. . 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

[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] TRA and Supplements can be found on CMS' internal website: http://cmsnet.cms.hhs.gov/hpages/oisnew/foffice/m/TRA.html (November 19, 2010).
[9] 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 QSSI. staff. Evidence to support any weaknesses discovered will consist primarily of screen prints, script output, and session data. MITRE will immediately notify CMS, And QSSI. staff if significant or immediately exploitable vulnerabilities are discovered during the assessment.

2 PLANNING

This section contains information describing the application 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 FEDERAL DATA SERVICES HUB BACKGROUND

2.1.1 Overview of the Marketplace Information Technology (IT) Systems

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.

2.1.3 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. ***Error! Reference source not found.*** depicts the basic Federal DSH concept.

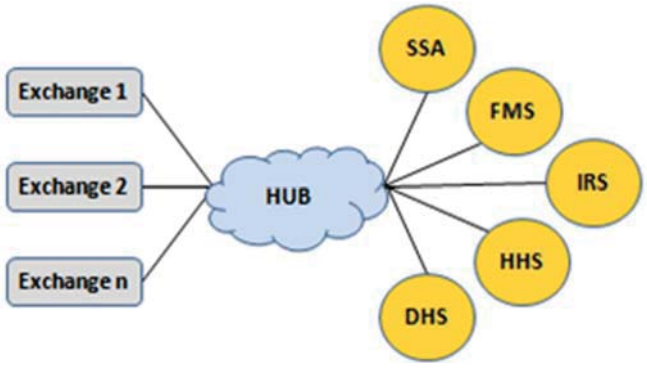


Figure 1: Federal Data Services Hub Concept

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
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.
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.

Business Process Name	Business Process Description
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.
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.

2.2 ASSESSMENT SCOPE

MITRE is tasked with providing a comprehensive SCA to determine if the Federal Data Services Hub (DSH) major application has properly implemented CMS security standards. According to

the System Security Plan (SSP), the FIPS 199 security categorization level for the DSH is (b)(5), (b)(6), (b)(7)c, (b)(7)e

SC Information About Persons = (b)(5), (b)(6), (b)(7)c, (b)(7)e
SC System Configuration Management Information = (b)(5), (b)(6), (b)(7)c, (b)(7)e
(b)(5), (b)(6), (b)(7)c, (b)(7)e
SC Other Federal Agency Information = (b)(5), (b)(6), (b)(7)c, (b)(7)e

The SCA will examine the management, operational, and technical controls that support the DSH to ensure adherence to the (b)(5), (b)(6), (b)(7)c, (b)(7)e security level specifications in the CMS ARS CMSR, PISP, BPSSM, and TRA. To adequately perform the SCA, MITRE anticipates that the MITRE Evaluation Team will be onsite for Monday August 19, 2013 through Friday August 30, 2013.

The scope of the SCA will be the (b)(5), (b)(6), (b)(7)c, (b)(7)e that is located in (b)(5), (b)(6), (b)(7)c, (b)(7)e (b)(5), (b)(6), (b)(7)c, (b)(7)e shall be the following:

- Documentation and interviews to encompass the Management and Operations of the DSH
- Databases (b)(5), (b)(6), (b)(7)c, (b)(7)e
- (b)(5), (b)(6), (b)(7)c, (b)(7)e with the DSH
- A sampling of the 34 VMs will be examined.
    - There is a base assumption that all the VMs are configured the same and therefore a sampling is sufficient
    - 30 VMS are running (b)(5), (b)(6), (b)(7)c, (b)(7)e
    - 4 VMS, are running (b)(5), (b)(6), (b)(7)c, (b)(7)e
- (b)(5), (b)(6), (b)(7)c, (b)(7)e interaction
- (b)(5), (b)(6), (b)(7)c, (b)(7)e

MITRE will also determine if DSH management and support personnel have an understanding of the CMS Information Security (IS) ARS including CMSR Version 1.5, *CMS Technical Reference Architecture*, *Version 2.1 (TRA)*, *United States Government Configuration Baselines (USGCB) and the NationalChecklist Program (NCP),*[10] CMS PISP, and BPSSM, as appropriate.

Application testing will be performed in the (b)(5), (b)(6), (b)(7)c, (b)(7)e adherence to the *CMS Information Security (IS) Assessment Procedure Version 2.0*[11] 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:

Comprehensive Scope Application SCA:

- Access Control (AC) , except AC-4, AC-16, AC-17, AC-18, AC-19, AC-20, and AC-CMS-1

[10] http://usgcb.nist.gov/ and http://web.nvd.nist.gov/view/ncp/repository.
[11] http://www.cms.hhs.gov/informationsecurity/downloads/Assessment_Procedure.pdf (March 19, 2009).

- Access Control (AC)
- Awareness and Training (AT)
- Audit and Accountability (AU)
- Security Assessment and Authorization (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)
- Risk Assessment (RA)
- System and Services Acquisition (SA)
- System and Communications Protection (SC)
- System and Information Integrity (SI)

2.3 ASSESSMENT ASSUMPTIONS/LIMITATIONS

MITRE has identified limitations of the planned assessment:

- The application being tested in the **PreProd** environment is functionally equivalent to the application deployed in the production environment.
- QSSI and IDL staff will provide timely responses to MITRE requests for information, access to systems to perform scans, testing and subject matter experts as documented in the SCA test plan.
- The MARS-E v1.0 is a subset of the CMSR, so the CMSR will cover the MARS-E v1.0.
- MITRE will not specifically evaluate the DSH against the IRS publication 1075 or Federal Tax Information (FTI).
- MITRE will collaborate with Booze Allen Hamilton (BAH) as needed and directed by GTL.
- **Out of Scope:**
  - (b)(5), (b)(6), (b)(7)c, (b)(7)e for system availability and performance
  - (b)(5), (b)(6), (b)(7)c, (b)(7)e build automation
  - (b)(5), (b)(6), (b)(7)c, (b)(7)e ode quality
  - (b)(5), (b)(6), (b)(7)c, (b)(7)e scanning tool
  - Jump Servers – covered by the Platform as a Service (PaaS)

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 July 31, 2013.

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 Configuration Manager

The Configuration Manager shall be able to describe the policy, processes, procedures, standards, and technical measures utilized for configuration management and change control in order to maintain a secure system baseline. The Configuration Manager shall be able to provide details of the application specific or system/enterprise configuration/change control processes and documentation, including identification, configuration/change management plan, status accounting, and audit procedures. The baseline could include, but is not limited to, software configuration, network infrastructure configuration, and application design and development resources. During the SCA process and onsite assessment, the Configuration Manager shall be available for interviews and to provide documentation under the Configuration Manager's responsibility.

2.5.6 Contingency Planning Manager

The Contingency Planning Manager develops the Contingency Plan for system recovery and works with the Business Owner and System Owner to determine the critical components and an appropriate system recovery strategy based on the business impact analysis, system recovery time objective (RTO), and recovery point objectives (RPO). The Contingency Planning Manager develops and maintains the Contingency Plan for the system, ensuring that testing of the plan is completed based on the organizational and business requirements. During the SCA process and onsite assessment, the Contingency Planning Manager shall be available for interviews and to provide the System Contingency Plan documentation and update process, system contingency testing schedule, and system contingency plan test reports.

2.5.7 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.

2.5.8 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.

2.5.9 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.

2.5.10 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.

2.5.11 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.

2.5.12 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, QSSI and IDL 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
Monique Outerbridge	CMS/OIS/CIISG	Business Owner
Darrin Lyles	CMS/OIS/CIISG	CMS Facilitator (Lead)
Hung Van	CMS/OIS/CIISG	CMS Government Task Leader
Denis Mirskiy/Murali Kotnana – (b)(5), (b)(6), (b)(7)c, (b)(7)e Denis Mirskiy/Rupinder Singh – (b)(5), (b)(6), (b)(7)c, (b)(7)e	QSSI	Database Administrator
Tom Schankweiler Darrin Lyles	CMS/OIS CMS/OIS	SSO ISSO
Bielski, Jim	MITRE	Lead Evaluator
Karlton Kim	QSSI	Project Manager
Jagadish Gangahanumaiah	QSSI	Deputy Project Manager
Balaji Gudi	QSSI	Syste (b)(5), (b)(6), (b)(7)c, (b)(7)e

Name	Organization	Role
Sid Telang Priya Aluru	QSSI	Release Manager – Development Release Manager - Production
David Holyoke	QSSI	Chief Architect
Kamesh Thota	QSSI	Security Architect
Dan McGuire	QSSI	Infrastructure Manager
Roy Mardis	QSSI	Infrastructure Configuration Manager
Mike Battles/Chris Mason	QSSI	Infrastructure Engineer (RH SME)

2.7 PHYSICAL ACCESS AND WORK AREA REQUIREMENTS

MITRE requires access to various systems, networks, infrastructure, and facilities. The MITRE Evaluation Team may requires network access to the Internet. For network scans, MITRE will review MITRE (b)(5), (b)(6), (b)(7)c, (b)(7)e provided by the infrastructure support contractor URS, and MITRE will perform independent testing as required. In addition, (b)(5), (b)(6), (b)(7)c, (b)(7)e available for review as part of the continuous monitoring program. To expedite and facilitate testing, each MITRE staff performing testing will utilize two laptops. 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 and telecommunication services for conducting interviews and analyzing data.

QSSI will provide the requested access and work facilities to MITRE at their offices located 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
Acronym: DSH

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, QSSI and IDL 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	
D02	System Security Plan (SSP) SSP Workbook	PL-2 System Security Plan CA-4 Security Certification	ILC Framework CMS PISP FISMA CMSR	
D03	Privacy Impact Assessment (PIA)	PL-5 Privacy Impact Assessment	ILC Framework CMSR	
D04	Contingency Plan	CP-2 Contingency Plan	ILC Framework CMSR	
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	
D07	Version Description Document (VDD)	SA-3 Life Cycle Support	ILC Framework CMSR	
D08	Interconnection agreements, Memorandum of	CA-3 Information System Connections	CMSR	

Document Element #	Document/Information Requested	ARS CMSR	Policy	Comments
	Understanding (MOU) and/or Interconnection Security Agreement (ISA)	SA-9 External Information System Services		
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	
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	May be documented in the SSP; verify that the level of detail is acceptable.
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	
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	
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	Not Applicable, inherited control from the 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	
D16	Open Corrective Action Plans (CAP) items from previous security controls assessments	CA-5 Plan of Action and Milestones (POA&M)	CMSR	When applicable

Document Element #	Document/Information Requested	ARS CMSR	Policy	Comments
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	
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	May be documented in the SSP
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	
D22	CMS Security Certification Form (if system previously authorized—TAB A)	CA-6 Security Authorization	CMSR	When applicable
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	

3.1.3 Script Output and Device Running Configuration Requirements

MITRE must obtain the database, and operating systems script output, 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

As there are no application-specific user accounts to test, MITRE will need to examine the configuration of and testing evidence, (b)(5), (b)(6), (b)(7)c, (b)(7)e Cases that have been accomplished to validate the proper configuration and use of (b)(5), (b)(6), (b)(7)c, (b)(7)e extensions. MITRE will need to review the WSDL's, and may need accounts to perform UI tests.

For the list of available Hub Web Services (WSDLs) MITRE will refere to (b)(5), (b)(6), (b)(7)c, (b)(7)e

Any futher testing that can be performed or demonstrated will be performed against (b)(5), (b)(6), (b)(7)c, (b)(7)e environment. Based on the defined assessment scope, the application roles and responsibilities/privileges are listed in Table 6, **Error! Reference source not found.**, **Error! Reference source not found.** and **Error! Reference source not found.**.

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

The following URL, (b)(5), (b)(6), (b)(7)c, (b)(7)e is required to access (b)(5), (b)(6), (b)(7)c, (b)(7)e Messaging.

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 Documentation Review

Prior to and during the assessment, the MITRE Evaluation Team will review documents provided by CMS, QSSI and IDL. The review will assess whether appropriate management and operational controls have been implemented; however, it will also be used to augment technical controls. For example, if the ARS CMSR stipulates that the password length for the information system is required to be eight characters and the SSP documents that the length of passwords is eight characters, the technical assessment will confirm whether passwords are configured to be eight characters in length. As a part of the assessment and when feasible, MITRE will evaluate the adequacy and completeness of the SSP, Information Systems Risk Assessment (IS RA), and Contingency Plan in accordance with CMS guidelines and provide feedback. In general, the MITRE Evaluation Team will review, but not be limited to, the following sample set of documentation: SSP, IS RA, and Contingency Plan. For the complete documentation list, refer to Section 3.1.1. During the onsite assessment, MITRE will provide written evaluations of the ISRA, SSP, and CP and use these evaluation documents as a basis for interview, discussion, and clarification.

3.2.2 Vulnerability Assessment Tools

MITRE will work with CMS, QSSI and IDL 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:

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

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

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. As much as possible, MITRE will avoid affecting out-of-bounds systems; however, tools may send non-standard network traffic, which could affect non-targeted (out-of-bounds) hosts if located on the same network. The effects of network-based tools will be contained within the in-bound portions of the target environment to the greatest extent possible.

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, architecture of transactional Web systems, and Web programming technologies (e.g., Hypertext Markup Language (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
- Identify system vulnerabilities based on the following items:
  - Architecture design and implementation
  - Improper, weak, or vulnerable configurations
  - Non-standard configurations
  - Published or known weaknesses, bugs, advisories, and security alerts about the 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
  - Evaluation of buffer overflow attacks
  - Evaluation of Trojan horse attacks
- Evaluation of Web application buffer overflow and password vulnerabilities by performing tests that include brute force password attacks and buffer overflow
- Perform network reconnaissance scanning to identify services (i.e., Telnet, file transfer protocol [FTP], etc.) that are available from targeted servers

- Conduct interviews with key staff to examine management, operational, and technical controls
- Examine documentation to ensure adherence to CMS policies and standards
- 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, CMS TRA 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:

- System architecture and development methodologies
- System security policies
- CM processes
- Patch management
- Audits and log analysis
- Contingency planning and backup and recovery

3.3.2 Observances

During the course of the assessment, the MITRE Evaluation Team will also scrutinize personnel and the physical environment, as applicable, to determine if security policies and procedures are being followed. Examples of areas that may be included are:

- If MITRE staff are issued visitor badges
- If any form of identification is requested prior to visitor badge issuance
- How employees label and discard output materials
- Are monitors positioned to prevent "shoulder surfing" or viewing from windows and open spaces
- If telecommunication and wiring closets are locked

While onsite and if appropriate, the MITRE Evaluation Team will also conduct a data center tour to determine whether physical controls securing CMS IS and data are adequate.

3.3.3 Configuration Review

During the assessment, the MITRE Evaluation Team will review switch, router, firewall, server and software configurations, and network and application architecture diagrams to determine if the controls delineated by the CMS ARS CMSR policies, CMS Minimum Security Configuration Standards for Operating Systems, and industry best practices (i.e., those outlined in the *Router Security Configuration Guide* published by the National Security Agency [NSA] and Defense Information Systems Agency [DISA] Security Technical Implementation Guides [STIG]) are being followed.

3.3.4 Application Testing

MITRE will test the DSH 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 or QSSI 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.

3.3.5 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 the results (b)(5), (b)(6), (b)(7)c, (b)(7)e to identify known flaws in the server version and settings
- Review database security configuration settings to determine if adequate system protections are implemented
- Interview the system and database administrators concerning database server configurations and security relevant mechanisms

4 REPORTING

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

4.1 SECURITY CONTROLS ASSESSMENT FINDINGS SPREADSHEET

The SCA findings spreadsheet (Table 7) 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.

Table 7. Findings Spreadsheet

Weakness	Risk Level	CMSR Security Control Family	Reference	Affected Systems	Easy/Difficult Fix	Est/Work Effort	Finding	Failed Test Description	Actual Test Results	Recommended Corrective Actions	Status
Wednesday September 1, 2010											

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,[12] MITRE will assign these values to each Business Risk. The risk ratings are described in Table 8.

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

Table 8. 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 9.

Table 9. 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

Rating	Definition of Ease-of-Fix Rating
	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 10.

Table 10. 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 QSSI.

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 (b)(5), (b)(6), (b)(7)c, (b)(7)e ulnerabilities 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, QSSI and IDL. The MITRE Evaluation Team will diligently respond to inquiries made by CMS, QSSI and IDL 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 , QSSI and IDL 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 11.

Table 11. MITRE Evaluation Team Points of Contact

Name	Position	Phone Number	Email Address
Jim Bielski	Lead Evaluator	(410) 402-2717	jbielski@mitre.org
Yi-Fang Koh	Database Evaluator	(703) 983-3995	kohy@mitre.org
To Be Identified	Application Evaluator		
Paul Klein	Firewall Evaluator	(703) 983-1062	pklein@mitre.org
Eugene Aronne	(b)(5), (b)(6), (b)(7)c, (b)(7)e Evaluator	(301) 429-2246	earonne@mitre.org
Barbara Stamps	(b)(5), (b)(6), (b)(7)c, (b)(7)e Evaluator	(703) 983-4556	bstamps@mitre.org
Carmella Thompson	Interviewer	(443) 934-0411	cthompson@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 12.

Table 12. CMS Points of Contact

Name	Position	Phone Number	Email Address
Jessica Hoffman	CMS/OIS GTL	(410) 786-4458 (O)	jessica.hoffman@cms.hhs.gov
Jason King	CMS/OIS GTL	(410) 786-7578 (O)	jason.king@cms.hhs.gov
Jane Kim	CMS/OIS/GTL	(443) 721-4064	jane.kim@cms.hhs.gov
Kirk Grothe	CMS Maintainer	(202) 407-3015	kirk.grothe@cms.hhs.gov
Hung Van	CMS Program Manager	(202) 510-6898	hung.van@cms.hhs.gov
Monique Outerbridge	Business Owner	(202) 465-5075	monique.outerbridge@cms.hhs.gov
Thomas Schankweiler	ISSO	301-875-1536	thomas.schankweiler@cms.hhs.gov

The QSSI POCs for the SCA are listed in Table 13.

Table 13. Vendor Points of Contact

Name	Position	Phone Number	Email Address
Karlton Kim	Program Manager	410-274-5835	kkim@qssinc.com
Kamesh Thota	Security Officer	571-294-9781	kthota@qssinc.com
Thomas Swoboda	HUB Architecture Team	(work through Kamesh)	tswoboda@qssinc.com
David Holyoke	HUB Architecture Team	(work through Kamesh)	dholyoke@qssinc.com
Dan McQuire	Operational Lead	(work through Kamesh)	dmcguire@qssinc.com

Name		Email Address
Thomas Peters-Hall	CM/Infrastructure team suport (b)(5), (b)(6), (b)(7)c, (b)(7)e	tpetersh (b)(5), (b)(6), (b)(7)c, (b)(7)e
Chris Mason	CM/Infrastructure tea suport (b)(5), (b)(6), (b)(7)c, (b)(7)e	cmason
Mike Battles	HUB Architecture Team, (b)(5), (b)(6), (b)(7)c, (b)(7)e (work through Kamesh)	mbattle

5.2 TECHNICAL STAFF REQUIREMENTS

CMS, QSSI and IDL 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, networks, infrastructures, facilities, and monitoring assessment activities.

5.3 ONSITE SCHEDULE

MITRE's onsite schedule can be found in Table 14. Joint refers to the the close coordination of testing with the Federally Facilitated Marketplace (FFM). Joint briefings will be conducted to save time.

Table 14. MITRE Onsite Schedule

Day / Date	Time	Meeting
Mon 8/19	10:00 – 11:00	**Joint** Kick off Meeting
	3:30 – 4:30	FFM DSH **Joint** SCA Daily Outbrief
Tue 8/20	9:30 – 11:00	DSH ISSO/Business Owner Interview
	11:00 – Noon	DSH Walk through / Demo
	1:00 – 2:00	DSH Contingency Planning/Disaster Recovery Interview
	2:00 – 3:00	DSH Configuration Manager Interview
	3:30 – 4:30	**Joint** SCA Daily Outbrief
Wed 8/21	9:30 – 11:00	DSH Database Administrator Interview
	3:30 – 4:00	**Joint** SCA Daily Outbrief
Thu 8/22	10:00 – 11:30	DSH Documentation Interview
	1:00 – 2:30	DSH Application Developer Interview
	3:30 – 4:00	**Joint** SCA Daily Outbrief
Fri 8/23	3:30 – 4:00	**Joint** SCA Daily Outbrief
Mon 8/26	10:30-Noon	(DSH) MIDAS (b)(5), (b)(6), (b)(7)c, (b)(7)e
Tue 8/27	3:30 – 4:00	FFM DSH **Joint** SCA Daily Outbrief
	9:30 – 11:00	(b)(5), (b)(6), (b)(7)c, (b)(7)e
	3:30 – 4:00	**Joint** SCA Daily Outbrief
Wed 8/28	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 15 describes the estimated timeline for assessment actions and milestones.

Table 15. Estimated Timeline for Assessment Actions and Milestones

Action/Milestone	Description	Date(s)
Provide scripts, data calls, or other requests to CMS	Lead evaluator provides the scripts, data calls or other requests for the Mainframe, Server O/S and Databases, when applicable	Monday July 22, 2013

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	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