Table of Contents: Exhibits

Exhibit 1 ..... **1**

Exhibit 2 ..... **5**

Exhibit 3 ..... **23**

Exhibit 4 ..... **35**

Exhibit 5 ..... **37**

Exhibit 6 ..... **39**

Exhibit 7 ..... **47**

Exhibit 8 ..... **80**

Exhibit 9 ..... **82**

Exhibit 10 ..... **100**

Exhibit 11 ..... **214**

Exhibit 12 ..... **338**

Exhibit 13 ..... **374**

Exhibit 14 ..... **441**

Exhibit 15 ..... **461**

Exhibit 16 ..... **465**

Exhibit 17 ..... **469**

Exhibit 18 ..... **471**

Exhibit 19 ..... **487**

Exhibit 20 ..... **490**

Exhibit 21 ..... **492**

Exhibit 22 ..... **505**

Exhibit 23 ..... **507**

Exhibit 24 ..... **511**

Exhibit 25 ..... **514**

Exhibit 1

E-mail from CMS staff to Senate Committee staff. Responding to questions from Senate Committee. April 22, 2013.

From: [redacted] (CMS/OL) [redacted]]
Sent: Tuesday, April 22, 2014 11:23 AM
To: Brandt, Kim (Finance); [redacted] (CMS)
Cc: Millspaw, Tegan (Judiciary-Rep); Bonelli, Anna (Finance)
Subject: RE: Follow-up questions for Henry

Hey Kim,

Thanks for your patience with us. Here are the responses to your questions. Let me know if you need anything else, [redacted]

1. **Mr. Chao stated that Kirk Grothe or Monique Outerbridge would have elevated any IV&V reports that were serious. Did anyone ever elevate an IV&V report finding to Mr. Chao? To anyone else?**

The purpose of the IV&V reports was to provide an objective assessment of Healthcare.gov's processes throughout the project's lifecycle. Therefore, part of the process for developing the IV&V reports was for TurningPoint to communicate with the project management team, including Henry Chao, about the developmental process of the products and potential risks or problems that could disrupt development. TurningPoint's analysis were sometimes not up-to-date, since they were not directly involved in the day-to-day development of the systems and were sometimes reviewing documents that were one to two months old as a result. Therefore, some of the issues identified in the TurningPoint reports may have already been resolved or mitigated, but those resolutions were not reflected in the reports.

The TurningPoint reports were one type of many different ongoing evaluations and assessments for the FFM. For example, the FFM was tested for functionality and security throughout the summer and fall of 2013. This testing was performed by CMS employees and contractors who were directly engaged in the day-to-day development of the systems. As we have said before, throughout September, CMS was working to continually test functionality of the website. The purpose of these tests was to identify areas that were not operating properly and work to resolve those issues.

2. **Please clarify the discussion we had about anonymous shopping and EIDM:**

    a. **Did disabling the Anonymous Shopping feature drive additional traffic to the EIDM?**

CMS officials disabled the Anonymous Shopping function in September because the function had significant defects, failed testing, and could not successfully complete essential functions. Disabling the Anonymous Shopping function did not drive additional traffic to the EIDM. All users would have been required to create accounts and verify their identities, with or without the Anonymous Shopping feature.

The Anonymous Shopper function, if it had been operational, also would have required consumers to create accounts. Since the shopper function being developed by CGI would have required consumers to submit some personally identifiable information to generate accurate price estimates, federal rules governing the security of information systems would have required the authentication of those user identities.

b. **QSSI reported that CMS did not direct QSSI to scale up the EIDM until launch. QSSI indicated that CMS's omission led to the EIDM feature being unable to handle the unexpectedly high traffic. Is this correct?**

No, as CMS has said before, as part of system testing, CMS identified that the EIDM system may experience capacity issues in the number of users who could create an account prior to October 1. In order to increase capacity, CMS added additional system hardware that would be able to handle the additional capacity needed.

However, after the launch on October 1, additional issues were identified related to infrastructure and hardware that caused problems with EIDM. Since October 1, CMS implemented several software changes and provided new infrastructure. As a result, EIDM performance significantly improved and individuals were able to move through account creation and registration quickly.

3. **The language in Amendment 0003 of QSSI's contract HHSM-500-2007-0002 states that all validation and implementation testing should be conducted independently (subsection J.1.10.1). However, QSSI representatives told us that they tested the hub themselves. Can you explain:**

   a. **Did QSSI test the data hub themselves, or was there also an independent tester? If so, which contractor performed independent testing?**

A separate contract and team within QSSI conducted the independent performance testing for the Hub. The contractors who tested the performance were not a part of the programming team.

Additionally, since the Hub is an integral tool needed to complete several eligibility and enrollment functionalities, it was tested throughout the test period for the FFM and was ran through several different test cases.

Also, the Hub completed its independent Security Controls Assessment, which was conducted by MITRE on August 23, 2013 and received an authorization to operate on September 6, 2013. The completion of this testing confirms that the Hub complies with federal standards and that HHS and CMS have implemented the appropriate procedures and safeguards necessary for the Hub to operate securely on October 1.

   b. **If not, why was QSSI permitted to perform testing of the software it developed?**

A separate contract and team within QSSI conducted the independent performance testing for the Hub. The contractors who tested the performance were not a part of the programming team.

From: Brandt, Kim (Finance) [redacted]
Sent: Wednesday, April 02, 2014 10:55 AM
To: [redacted] (CMS); [redacted] (CMS/OL)
Cc: Millspaw, Tegan (Judiciary-Rep); Bonelli, Anna (Finance)
Subject: Follow-up questions for Henry

[redacted] – We had just a couple of follow up questions for Henry from our discussion with him a few weeks ago. If you could pass along to him and provide us with his answers it would be much appreciated. Thanks! Kim

1. Mr. Chao stated that Kirk Grothe or Monique Outerbridge would have elevated any IV&V reports that were serious. Did anyone ever elevate an IV&V report finding to Mr. Chao? To anyone else?
2. Please clarify the discussion we had about anonymous shopping and EIDM:
    a. Did disabling the Anonymous Shopping feature drive additional traffic to the EIDM?
    b. QSSI reported that CMS did not direct QSSI to scale up the EIDM until launch. QSSI indicated that CMS's omission led to the EIDM feature being unable to handle the unexpectedly high traffic. Is this correct?
3. The language in Amendment 0003 of QSSI's contract HHSM-500-2007-0002 states that all validation and implementation testing should be conducted independently (subsection J.1.10.1). However, QSSI representatives told us that they tested the hub themselves. Can you explain:
    a. Did QSSI test the data hub themselves, or was there also an independent tester? If so, which contractor performed independent testing?
    b. If not, why was QSSI permitted to perform testing of the software it developed?

Exhibit 2

FEPS IV V Executive Status Meeting. PowerPoint presentation. TurningPoint. July 17, 2013.

FEPS IV&V
EXECUTIVE STATUS MEETING

July 17, 2013

Prepared By:

TurningPoint

TurningPoint Global Solutions
Software Services Company™

Agenda

- CAP
  - Assessment Summary
  - CAP Tracker
  - Responses
  - Pending Responses
  - Remediation Efforts
- Assessment Highlights
  - Cloud Computing
  - Readiness Reviews
- Proposed Scope for Next Assessment
- Project Status
- June 2013 GAO Report
- Next Steps

7

CAP - Assessment Summary

Assessment #	Assessment Completion Date	Assessment Description	Total Findings	Total Low Findings	Total Moderate Findings	Total High Findings
1	9/7/2012	FFE/DSH/MIDAS: Evaluate Processes	103	25	48	30
2	12/14/2012	FFE/DSH/MIDAS/State Engagements/Operational Oversight (Governance): Evaluate Processes	175	15	123	37
3	2/15/2013	FFE/DSH Code Evaluation	52	5	32	15
		MIDAS/State Engagements/Governance: Evaluate Processes	44	10	33	1
4	3/5/2013	XOC: Evaluate Processes	56	16	34	6
5	3/29/2013	zOne: Code Evaluation	14	0	9	5
6	4/19/2013	FFE: QHP RTM Traceability	19	4	7	8
		State Engagements: Evaluate Training Materials	24	13	9	2
		Testing Playbook: Evaluate Processes	28	4	17	7
7	5/22/2013	IMS: Evaluate IMS Components	35	9	21	5
8	6/12/2013	Cloud computing: Evaluate Processes	51	10	29	12
9	7/12/2013	Readiness Reviews: Evaluate Processes	8	4	3	1
		Total Findings	**609**	**115**	**365**	**129**

Developed an automated process for managing the CAP Lifecycle in CALT Tracker
https://calt.cms.gov/sf/tracker/do/listArtifacts/projects.cms_ois_feps_iv_v/tracker.iv_v_corrective_action

Management can run reports at their convenience

CAP Tracker - Screenshot

Search Tracker

IV&V Corrective Action Summary

Open by priority

Open Vs Closed

Assessment Number	Artifact ID : Title	Task Item	Description	System	Action	Contractor	Responsible Individual	Risk Level	Status	Date Closed
				Any		Any	Any	Any	All Ope	Any
		Database Design: DM-5	Recommend improvements to existing schema to improve data integrity and system performance.	DSH/HE	5/1/2013 DSH: No detailed database design documents found.	QSSI/KGI	QSSI: Karlton Kim/CMS: Monica Winthrop	High	Open	

FEPS IV&V

CAP - Response Summary

Assessment #	Assessment Description	Assessment Stakeholder Responses				
1	Release 2 - FFE/DSH, MIDAS	FFE	DSH	MIDAS		
2	Release 3 - FFE/DSH, MIDAS Phase 1, State Engagements	FFE	DSH	MIDAS	State Engagements	Governance (Due Date: 6/13/2013)
3	FFE/DSH Code Evaluation, State Engagements, Release Documentation	FFE	DSH	MIDAS	State Engagements	Governance
4	XOC Documentation	XOC Governance	XOC Documentation			
5	Zone Code Evaluation	DSH (Due Date: 8/9/2013)				
6	QHP Traceability, Playbook, State Engagements	FFE	Playbook (Due Date: 6/28/2013)	State Engagements		
7	Integrated Master Schedule Components	DPMG (Due Date: 6/28/2013)				
8	Cloud Computing	Terremark (Due Date: TBD)				
9	Readiness Review	DPMG (Due Date: TBD)				

IV&V Review Complete

Awaiting Response

Response Received; Pending Review

Partial Responses Received; Pending Review

CAP – Pending Responses [Placeholder]

11

CAP - Remediation Efforts – As of 7/10/2013

- Closed **42.85%** of the findings (261 out of 609)
- Breakdown of the Review:

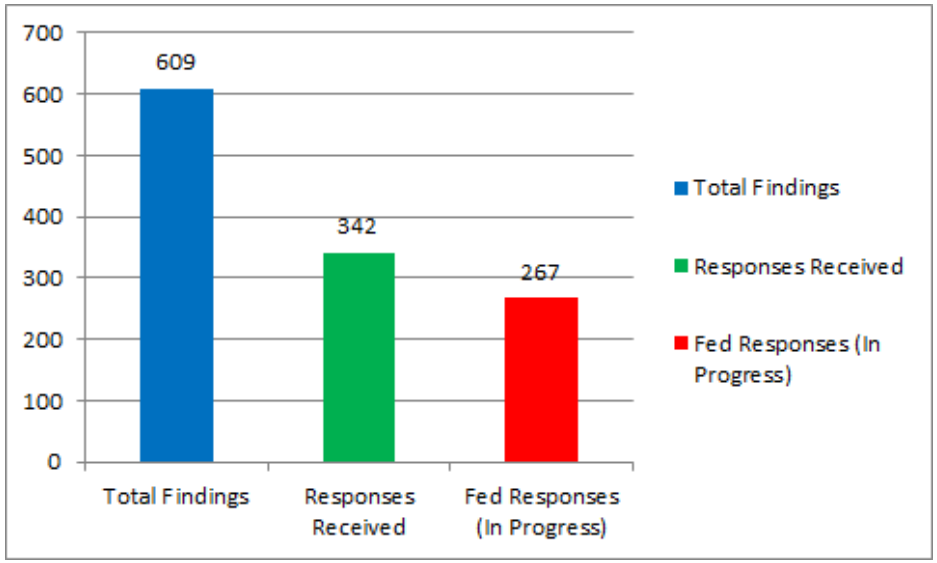
Assessment #	Total	Closed	Open
Assessment 1	103	95	8
Assessment 2	175	110	65
Assessment 3	96	56	40
Sub Total	374	261	113
Assessment 4	56	0	56
Assessment 5	14	0	14
Assessment 6	71	0	71
Assessment 7	35	0	35
Assessment 8	51	0	51
Assessment 9	8	0	8
Total Findings	609	261	348

- Requested additional documentation to revisit remaining 113 findings through Assessment #3
- Currently reviewing documentation for Assessment #4

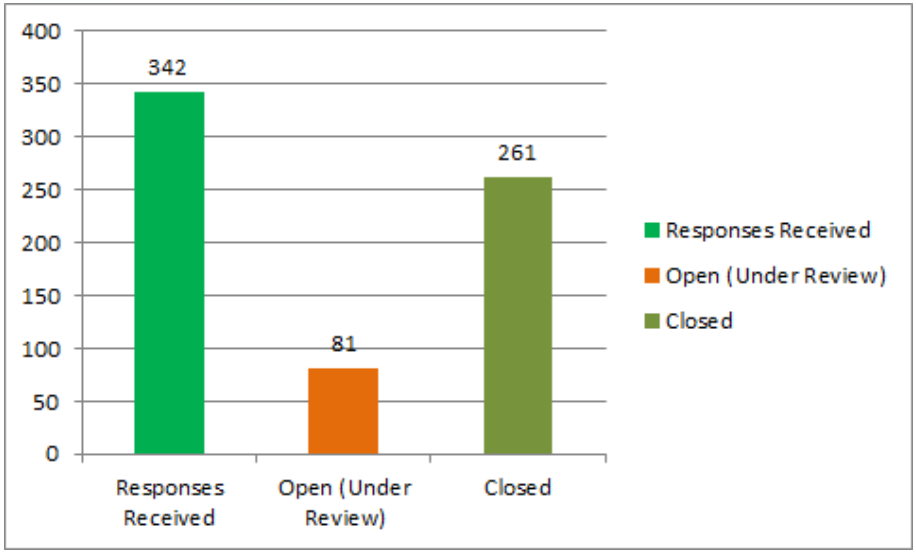
12

CAP - Remediation Efforts (Contd..)

Assessment Response Statistics



Assessment Remediation Status



Assessment Highlights – Cloud Computing

Scope of Service	SOW Task #
Requirements Management (RM)	RM-6, RM-7, RM-8, RM-9, RM-12
Operating Environments (OE)	OE-1, OE-2 , OE-3, OE-4, OE-5,
	OE-6, OE-10, OE-11, OE-12 , OE-13
System and Acceptance Test (SAT)	ST-11, ST-15
Operations Oversight (OO)	OO-1, OO-2, OO-4, OO-5, OO-6

Findings Summary

Total Findings				
	Low	Moderate	High	Total
IV&V Service Area				
Requirements Management	4	7	3	14
Operating Environment	3	12	4	19
System and Acceptance Testing	0	0	0	0
Operations Oversight	3	10	5	18
Total	**10**	**29**	**12**	**51**

14

Cloud Computing - Key Findings

- **Requirements Management**
  - Asigra tool not upgraded to provide consolidated reports for cloud backups.
  - Miami (DR Failover site) does not have enough processors, memory, storage allocated to meet the 24/7 operating requirement in the SOW.
- **Operating Environment**
  - Current hardware server configurations and related processes appear to be inadequate.
  - The current Cloud infrastructure (i.e., hardware) has deviated from the defined and approved security policy as detailed in the Terremark SOW.
  - The existing capacity planning is not adequate.
  - The system's capacity to support future growth cannot be verified.
- **Operations Oversight**
  - Multiple artifacts in CALT under CMS OIS ECloud Support are not implemented in accordance with the SLAs.
  - Consolidated 3 ITIL Processes (Event, Incident, Problem) into 1 process instead of having separate processes.
  - The Release Management process is not being followed.
  - IaaS problems (root cause of an incident) are not tracked consistently.

Cloud Computing - Key Recommendations

- ***Capacity*** - CMS and relevant contractors should carry out a capacity planning lifecycle to address the current business requirements and to also forecast future processing requirements.
- ***Security*** - Ensure Plan of Action and Milestones (POAMs) are met by the due date and take steps immediately to mitigate residual security risk.
- ***Disaster Recovery*** - Provide a failover site with the same configuration as the primary site to meet 24x7 operations.
- ***Backup*** - Review the backup and recovery procedures, make decisions on which method should be used and update the documents to ensure files are consistent in backup/restore methodology.
- ***Incident Management*** - Update section 4 of the Incident Management Plan including the trend analysis process, communication process among the teams that must pool their knowledge and expertise to diagnose and resolve the problem, and the process for setting up priority levels to ensure there is efficient allocation of resources.

Cloud Computing – Henry's Questions

- **Architecture**
  - The infrastructure is scaleable and software adheres to the FEA and CMS TRA.
  - Capacity is inadequate: evidenced in hardware server and VM shortages.
- **Network Layer**
  - Dynamic network throttling services are not available; fixed increments have to be purchased.
  - Network monitoring is available for 5 months, for highest burst, total data.
- **Monitoring and provisioning operations**
  - Capacity planning is inadequate: no formulas, models, methods; missing inputs.
  - Change request process is complete; SLAs appear to be not met, but may be bumped in priority, some TBDs still present in SLA.
  - Backup requirements and schedules are inconsistent.
  - Problem, incident and event management processes are managed as one process.
  - No centralized Configuration Management Database
- **Disaster Recovery**
  - Insufficient processors, memory and storage to meet 24 x 7 operations of FMPS applications in October.

Assessment Highlights – Readiness Review (Findings & Recommendations)

- **Operations Oversight**
  - X.
  - Y.
  - Z.

Scope for Next Assessment

- Full Life Cycle Evaluation – FFE/DSH
- Testing Playbook Implementation

Project Status – Tasks Accomplished & Proposed Priorities

Tasks Accomplished	Assessment Completion Date	Tasks to be Accomplished - Assessments	Estimated Completion Date
1. Cloud Computing	6/12/2013	6. Full Life Cycle Evaluation – FFE/DSH	9/6/2013
2. Readiness Review (Mini-Assessment)*	7/12/2013	7. Playbook Implementation	9/6/2013
		8. Full Life Cycle Evaluation - MIDAS	10/31/2013
CAP Remediation Tasks - On-going		9. State Engagements	12/31/2013
3. CAP Remediation (Assessments 1 through 6)		10. Remedy & XOC	1/31/2014
4. Continuous CAP Remediation Follow-up		11. SHOP Traceability	3/15/2014
5. CAP Remediation (From Assessment # 7 onwards)		12. CO-OP	5/14/2014
* Special Request			

- TurningPoint is still awaiting Mod for the above referenced tasks; Mod is under OAGM's review

June 2013 GAO Report Highlights

- A
- B
- C

Next Steps

- Gain consensus on the proposed priorities

22

Exhibit 3

Email from Jeffrey Grant to Sharon Arnold. July 8, 2013. Obtained from House Energy & Commerce Committee

Unknown

From: Calem, Mark (CGI Federal)[redacted]

Sent: Tuesday, July 09, 2013 10:15 AM

To: Chao, Henry (CMS/OIS); Grothe, Kirk A. (CMS/OIS); Oh, Mark U. (CMS/OIS); Manambedu, Lakshmi (CGI Federal); Van, Hung B. (CMS/OIS); Couts, Todd (CMS/OIS)

Cc: Outerbridge, Monique (CMS/OIS); Murray, Ruairi S. (CMS/OIS); Berkley, Katrina (CMS/OIS); Rhones, Rhonda D. (CMS/OIS)

Subject: RE: IT support for PPFG

Importance: High

Henry,

I met with the FM team to get a better understanding of the issues that Jeff brought up. While I can understand some of Jeff's concerns, there is a bigger picture around where we stand with FM and our plans to get the work done.

- We do have a separate team for FM which stands at 24 FTE's, including 11 developers and 3 architects). This team is focused on only FM tasks
- We did have to move a few of the staff to PM & E&E to balance competing priorities, but for the FM staffing levels were commensurate with planned size of the team per the budget. Having said this, we are planning on adding 11 additional staff given the new SOW to support all of the FM tasks – some of which have already started.
- In terms of the five tracks:
  - We are working diligently on the SBM data collection / advanced CSR date calculation. This is the first FM component to go live we are working through some initial build/deploy/integration challenges. The timeframe was accelerated and we have just received a new CR that has thrown a wrinkle into the solution. But we are working through it. From my last report, there are two critical defects outstanding that are being addressed.
  - HIGLAS Integration is on target. However, we still don't have all of the requirements for Bookkeeping and we are facing some challenges where prior decisions are being re-opened.
  - Payee/banking data collection slated for 9/16 is tight – and we plan to add additional staff to support development activities. We would like to discuss this target date as it is in the middle of preparing E&E for open enrollment and this data isn't needed for operations until December 2nd.
  - APTC/CSR/user fee monthly payment calculation is not an October 1 item and we have not placed a high priority on it.
  - Edge Server initial deployment does present a challenge since it is true that the key resource that was leading this effort is fully engaged with SBM data collection. This has hampered our ability to hold some technical meetings during the past few weeks – but we have supported the majority. We will restart our focus on this, but we need to discuss overall capabilities – since we think there are some features that are not essential for the initial deployment.

As we have discussed before, we are working through program-wide priorities, but we understand the timelines and importance of the FM tasks and are working hard to complete them. Please let me know if you have any questions.

Thanks, Mark

Mark Calem | Vice President, Consulting | CGI Federal
[redacted]

From: Chao, Henry (CMS/OIS)[redacted]
Sent: Monday, July 08, 2013 7:29 PM
To: Calem, Mark (CGI Federal); Grothe, Kirk A. (CMS/OIS); Oh, Mark U. (CMS/OIS); Manambedu, Lakshmi (CGI Federal); Van, Hung B. (CMS/OIS); Couts, Todd (CMS/OIS)
Cc: Outerbridge, Monique (CMS/OIS); Murray, Ruairi S. (CMS/OIS); Berkley, Katrina (CMS/OIS); Rhones, Rhonda D. (CMS/OIS)
Subject: Re: IT support for PPFG

I just talked to Jeff and he understands things needed to shift between priority items. I don't think he was saying he would be willing to sacrifice E&E so that FM could show progress that was not priority.

It would be good to Respond to Jim though since Jeff has raised his concerns. Thanks.

Henry Chao
Deputy Chief Information Officer and Deputy Director
Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Blvd
Baltimore, MD 21244
[redacted]

From: Calem, Mark (CGI Federal)[redacted]
Sent: Monday, July 08, 2013 07:19 PM
To: Chao, Henry (CMS/OIS); Grothe, Kirk A. (CMS/OIS); Oh, Mark U. (CMS/OIS); Manambedu, Lakshmi (CGI Federal)[redacted]; Van, Hung B. (CMS/OIS); Couts, Todd (CMS/OIS)
Cc: Outerbridge, Monique (CMS/OIS); Murray, Ruairi S. (CMS/OIS); Berkley, Katrina (CMS/OIS); Rhones, Rhonda D. (CMS/OIS)
Subject: RE: IT support for PPFG

Henry, message received....i am on top of this and will get you a response ASAP.

Mark

Mark Calem | Vice President, Consulting | CGI Federal
[redacted]

From: Chao, Henry (CMS/OIS)[redacted]
Sent: Monday, July 08, 2013 6:32 PM
To: Grothe, Kirk A. (CMS/OIS); Oh, Mark U. (CMS/OIS); Manambedu, Lakshmi (CGI Federal); Calem, Mark (CGI Federal); Van, Hung B. (CMS/OIS); Couts, Todd (CMS/OIS)
Cc: Outerbridge, Monique (CMS/OIS); Murray, Ruairi S. (CMS/OIS); Berkley, Katrina (CMS/OIS); Rhones, Rhonda D. (CMS/OIS)
Subject: RE: IT support for PPFG

Replying to include others...

Henry Chao
Deputy CIO & Deputy Director,
Office of Information Services

Centers for Medicare & Medicaid Services
[redacted]

From: Chao, Henry (CMS/OIS)
Sent: Monday, July 08, 2013 6:30 PM
To: Grothe, Kirk A. (CMS/OIS); Oh, Mark U. (CMS/OIS); Lakshmi Manambedu [redacted] Calem, Mark (CGI Federal) [redacted] Van, Hung B. (CMS/OIS)
Cc: Outerbridge, Monique (CMS/OIS); Murray, Ruairi S. (CMS/OIS)
Subject: FW: IT support for PPFG
Importance: High

Can you get me a response on this to refute what Jeff is saying?

Henry Chao
Deputy CIO & Deputy Director,
Office of Information Services
Centers for Medicare & Medicaid Services
[redacted]

From: Kerr, James T. (CMS/CMHPO)
Sent: Monday, July 08, 2013 6:01 PM
To: Chao, Henry (CMS/OIS)
Cc: Grothe, Kirk A. (CMS/OIS); Lorenz, Samara A. (CMS/CCIIO)
Subject: IT support for PPFG
Importance: High

Henry, We need to discuss at your earliest convenience. Thanks, Jim

James T. Kerr
James T. Kerr, acting Deputy Director, Operations, CCIIO and Consortium Administrator CMHPO | Centers for Medicare and Medicaid Services [redacted]

From: Arnold, Sharon B. (CMS/CCIIO)
Sent: Monday, July 08, 2013 3:30 PM
To: Kerr, James T. (CMS/CMHPO)
Cc: Lorenz, Samara A. (CMS/CCIIO); Iyer, Raj (CMS/CCIIO; Grant, Jeffrey (CMS/CCIIO); Russell, Brigid M. (CMS/CCIIO); McWright, Laurie (CMS/CCIIO); Arnold, Grace C. (CMS/CCIIO)
Subject: FW: IT support
Importance: High

Jim,

I am forwarding an email from Jeff Grant outlining significant concerns with the FM build. Throughout this process, we had been assured by OIS that we had a separate development team working on FM issues, and the delay and issues surrounding the PM and E&E build would not impact our development. Even though some of our developers had been "loaned" to the PM team to help with their development for a short time, we were assured that our CGI resources would be protected. It now seems that there is a significant resource

issue impacting the FM build, and as far as we can tell our FM liaison from OIS (Walt Dunick) is just learning of this as well.

We will continue to work through this issue and streamline and prioritize where we can. We wanted you to be aware, in case you wanted to raise this with Henry Chao.

sharon

Sharon B. Arnold, Ph.D.
Director, Payment Policy and Financial Management Group
CCIIO
[redacted]

INFORMATION NOT RELEASABLE TO THE PUBLIC UNLESS AUTHORIZED BY LAW: This information has not been publicly disclosed and may be privileged and confidential. It is for internal government use only and must not be disseminated, distributed, or copied to persons not authorized to receive the information. Unauthorized disclosure may result in prosecution to the full extent of the law.

From: Grant, Jeffrey (CMS/CCIIO)
Sent: Monday, July 08, 2013 3:15 PM
To: Arnold, Sharon B. (CMS/CCIIO)
Cc: Russell, Brigid M. (CMS/CCIIO)
Subject: IT support

We just got off an extended set of development planning meetings with OIS. Suffice to say, the upshot is that the FM build appears to be way off track and getting worse. we also finally were told that there are only 10 developers total working on the FM build for all functionality. Only one of these developers is at a high enough skill level to handle complex issue resolution, which now appears to be required for all aspects of our build. With these limited resources, CGI is supposed to be developing on five tracks right now:

1. SBM data collection/advance CSR rate calculation
2. HIGLAS integration
3. Payee/banking data collection
4. APTC/CSR/user fee monthly payment calculation
5. Edge server initial deployment

Our SBM data collection effort is weeks behind schedule with most of the CGI test cases failing. Due to coordination issues between CGI and QSSI (as independent testing contractor), there has been no independent testing and CGI still cannot support user acceptance testing (originally scheduled for early June). We are one week out from production deployment, and we are being told already that it doesn't work. Furthermore, there is much functionality that was not yet completed that will either go in a "hot fix" for late July or into the 8/15 release.

HIGLAS integration will be barebones at best when we get to the early August integration test. There was some early development done last year that helps out this effort, but much remains to be accomplished in order to start integration testing with OFM next month. CGI expects to go into testing with the hub in mid July, but given the status of SBM data collection, this looks like a highly ambitious date. Since all transactions must go through the hub translator, this integration test is a critical success factor for the overall development.

Payee/banking data collection module is a user interface module that has 10 UI screens. None of the screens are developed. The developer for this piece left CGI and they are working on a replacement. This piece is

supposed to go into production 9/15. Needless to say it is in jeopardy.

Edge server, scheduled for full deployment 9/2, has not gone back into development. Although it has been through Beta test and functionality does exist, there are several critical items that need to be addressed prior to our go-live of 9/2. CGI scheduled a series of meetings to finalize the design for the 9/2 release. Some of these meetings have been completed as scheduled, but others have been canceled, including the one scheduled for this afternoon. CGI initially said that they did not have a list of items for discussion. When we pressed CGI about why we were not meeting when we are about a month out from testing and no development has started, CGI said that they had insufficient resources to cover this subject given the problems with the SBM deployment.

APTC/CSR/user fee monthly processing is not yet in development. Given the previous issues, it is hard to say when this work will go into development.

So while OIS has always said we had an independent team for FM development, they have never revealed the seriously substandard level of staffing that this team has. We believe that our entire build is in jeopardy. I think we need to consider which items in our build will not be done if we don't get substantially greater staffing levels.

Jeff Grant
Centers for Medicare & Medicaid Services
Center for Consumer Information and Insurance Oversight
Payment Policy and Financial Management Group
[redacted]

Unknown

From: Chao, Henry (CMS/OIS)

Sent: Saturday, July 20, 2013 7:55 AM

To: Cheryl Campbell; Bikram Bakshi; Chris Drumgoole; Par Rachakonda - US; Outerbridge, Monique (CMS/OIS); Oh, Mark U. (CMS/OIS); Grothe, Kirk A. (CMS/OIS)

Cc: Karlton Kim; Laura Fasching; Calem, Mark (CGI Federal); Lakshmi Manambedu; M Finkel BB; Van, Hung B. (CMS/OIS); Donohoe, Paul X. (CMS/OIS); Couts, Todd (CMS/OIS); Rhones, Rhonda D. (CMS/OIS); Berkley, Katrina (CMS/OIS); Rich Martin; Alan Koch; Geraldine Clawson; rich. schwarzkopf; [redacted] Ari Knausenberger; Radcliffe, Glenn D. (CMS/OIS); Joann Davis; 'Brian Paget'; Kash Badami; Thurston, Robert (CMS/CTR); Um, Peter (CMS/CTR); Igor Rafalovich; Riyaz Momin; Timothy Andrews; Mike Oelrich; Alicia Anderson; Stanley Rowen; Margush, Doug C. (CMS/OIS); Dill, Walter (CMS/OIS); Dunick, Walter T. (CMS/OIS); Lazenby, Daniel (CMS/OIS); Burke, Sheila M. (CMS/OIS); Schmidt, Donna W. (CMS/OIS); Adkins, Laura J. (CMS/OIS)

Subject: House Oversight and Government Reform Committee - Evaluating Privacy, Security, and Fraud Concerns with ObamaCare's Information Sharing Apparatus

Importance: High

Below are information and links to the Congressional Hearing Marilyn Tavenner and I attended this past Wednesday.

I am not sharing this with you because I think it's entertaining and informative. I wanted to share this with you so you can see and hear that both Marilyn and I under oath stated we are going to make October 1st. I would like you put yourself in my shoes standing before Congress, which in essence is standing before the American public, and know that you speak the tongue of not necessarily just past truths but the truth that you will make happen, the truth that is a promise to the public that millions of people depend on for us to make happen.

Aside from the political rhetoric, ranting, etc. my perspective is that on a personal and professional basis I made this promise on behalf of all of us and I have no doubt together we will drive the outcomes that flow from this promise.

Everyone in this email is a leader in this endeavor and I thank you for the support and vigilance in maintaining this promise that I speak of. I ask that you all take it every bit as serious as I do every minute of each day and in fact I will depend on it since much of my time going forward will be spent on Capitol Hill.

Please share this up, down, and wide so everyone will know not just what I promised on their behalf, but also to know that I am a true believer in our collective talents and commitment to change the world we live in and improve the lives of real people.

Thank you.

Henry Chao
Deputy CIO & Deputy Director,
Office of Information Services
Centers for Medicare & Medicaid Services

[redacted]

The included link is to a C-SPAN video of the hearing.

http://www.c-spanvideo.org/program/CareInfor

House Oversight and Government Reform Committee

Wednesday July 17,2013 | 10:00 a.m. in 2154 Rayburn House Office Building

http://oversight.house.gov/hearing/evaluating-privacy-security-and-fraud-concerns-with-obamacares-information-sharing-apparatus/

Witnesses

The Honorable Danny Werfel

Principal Deputy Commissioner

Internal Revenue Service

The Honorable Marilyn B. Tavenner

Administrator

Centers for Medicare and Medicaid Services

U.S. Department of Health and Human Services

Mr. Henry Chao

Deputy Chief Information Officer

Deputy Director of the Office of Information Services

Centers for Medicare and Medicaid Services

U.S. Department of Health and Human Services

Mr. Alan R. Duncan

Assistant Inspector General for Security and Information Technology Services

Treasury Inspector General for Tax Administration

Unknown

From: Chao, Henry (CMS/OIS)
Sent: Tuesday, July 16, 2013 10:07 AM
To: Outerbridge, Monique (CMS/OIS)
Cc: Murray, Ruairi S. (CMS/OIS); Grothe, Kirk A. (CMS/OIS); Berkley, Katrina (CMS/OIS); Oh, Mark U. (CMS/OIS); Van, Hung B. (CMS/OIS); Rhones, Rhonda D. (CMS/OIS)
Subject: RE: CGI Monthly Meeting Next Week
Importance: High

Did you see my other email about first just talking to [redacted] to convey just how low the confidence level and then pile on top of that the request for more money when we constantly struggle to get a release done, vacillating on delivery by due dates, and worse of all poor QA from build of the VMs all the way up to their software. They are the Prime and take direction from us so I don't want to hear about Marklogic, TMRK/URS, or anything elase. I just need to feel more confident they are not going to crash the plane at take-off, regardless of price.

Figure out how to get that conversation conducted and message conveyed.

Henry Chao
Deputy CIO & Deputy Director,
Office of Information Services
Centers for Medicare & Medicaid Services
[redacted]

From: Outerbridge, Monique (CMS/OIS)
Sent: Tuesday, July 16, 2013 10:02 AM
To: Robinson, Carolyn E. (CMS/OIS); Trenkle, Tony (CMS/OIS); King, Terris (CMS/OIS); Chao, Henry (CMS/OIS); Grothe, Kirk A. (CMS/OIS)
Cc: Shippy, Scott (CMS/OIS); Lewis, Melinda (CMS/OIS); Tierney, Janet L. (CMS/OIS); Blondell, Star (CMS/OIS); Weiss, Paul (CMS/OIS)
Subject: RE: CGI Monthly Meeting Next Week

I'm going to check with Mary to see if we can reschedule. Henry and I both will be in DC tomorrow and based on how Kirk looks and feels today I suspect he may not be in tomorrow.

From: Robinson, Carolyn E. (CMS/OIS)
Sent: Friday, July 12, 2013 12:11 PM
To: Trenkle, Tony (CMS/OIS); King, Terris (CMS/OIS); Chao, Henry (CMS/OIS); Grothe, Kirk A. (CMS/OIS)
Cc: Outerbridge, Monique (CMS/OIS); Shippy, Scott (CMS/OIS); Lewis, Melinda (CMS/OIS); Tierney, Janet L. (CMS/OIS); Blondell, Star (CMS/OIS); Weiss, Paul (CMS/OIS)
Subject: CGI Monthly Meeting Next Week

There is a CGI monthly meeting next week. Some information you all will want to know is that they need about $38 million more to get them through Feb 2014. CIISG is reviewing the proposal, and they will be getting back, to Paul Weiss, by next Thursday. This $38 does not include the approximate $40 million we have in the budget for this contract.

Kirk, you will want to weigh in with any technical points you want to make.

PM Deployment: Schedule Impact of Slippages

- **PM Deployment Slippages:**
  - Plan Transfer and Plan Preview Initially Scheduled for 7/15
  - Latest Status and Plans:
    - PM (FFM & Hub) – Impl & Prod: for Plan Transfer attempted on 7/22
    - FFM deployment to implementation was completed but regressions testing identified issue with Drug templates. Prod deployment was called off for FFM and Hub given that two needs to stay in synch
    - Plan Transfer going into production 7/23 - NAIC has been notified of our status.
    - Plan Preview UAT initially scheduled for 7/23 but potentially pushed back by a day to 7/24

- **Schedule Impact:**
  - Schedules for upcoming releases 7/31, 8/15 (Deferred PM Functions) may be compressed and under pressure since the same resources may be needed
  - Shorter testing times for upcoming Production and Test Deployments because of the extra effort in splitting 7/15 release into multiple mini-releases – additional DEV, TEST and IMPL cycles
  - Splitting releases increases regression testing cycles and possibility of errors, causing compression of other releases that come after them

CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES
OFFICE OF INFORMATION SERVICES

1

FM Releases : Schedule Impact of Slippages

- **FM Release Slippages:**
  - CSR Calculations – SBM Data Initially Scheduled for 7/15
  - Final CSR planned for 8/15
  - Latest Status and Plans:
    - FM (FFM) – Test: for fixes related to pulling data from URR, FFM, and creating a CSR report attempted on 7/22
    - FFM deployment to fix severity issues related to data pull (from URR and FFM-PM modules) as well as CSR calculation report did not yield planned results. CGI is troubleshooting.
    - Now being pushed to 7/31 (7/27 Saturday Actual date but now that slipped by a day to 7/28 Sunday)
- **Schedule Impact**:
  - Schedules for 8/15 release may be compressed and under pressure if any more slippages occur

CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES
OFFICE OF INFORMATION SERVICES

E&E Test Releases : Schedule Impact of Slippages

- **E&E Test Deployment 7/15 Slippages:**
  - Initial Release targeted for 7/15
  - Latest Status and Plans:
    - E&E (FFM) – Prod': for fixes related to Direct Enrollment web services and FFM application workflow attempted on 7/22
    - FFM deployment included updates to the Individual Application to ensure existing break in workflow has been corrected, deploy Direct Enrollment services, and fix 834 trigger in plan compare. For the most part, intended deployment results were obtained. However, we are seeing an issue in Plan Compare where session is getting lost (which effectively ends the workflow but does not impact Direct Enrollment testing).
    - My Account – Individual (Pages) – shifted to 7/31
    - My Account – Individual (Services) – shifted to 7/31
    - Enrollment - Create ESD (Services) – shifted to 7/31 and 8/30
    - Call Center Integration (Services) – shifted to 7/31
    - Plan Compare – Dental Screening Questions (Services) – Shifted to 7/31
    - Individual Application – General (Services) & Get Started (Pages) – Shifted to 8/15
    - Secondary Layering (UI) (Pages) – Shifted to 8/15 and 8/30
- **Schedule Impact:**
  - Shorter Issuer testing time windows – originally planned for 7/19 and now might be 7/24
  - Short testing windows may impact Quality if Day 1 functionality is being developed all the way up to 8/31 and 9/15
  - Cascading slippages may occur. If functionality planned for July slip, it may cause slippages in August where a lot more functionality is already planned.

CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES
OFFICE OF INFORMATION SERVICES

Exhibit 4

Email from Lori Stone of CGI to undisclosed recipients. July 27, 2013.

Name	% Complete
FFM	51%
Eligibility and Enrollment	53%
Financial Management	17%
Plan Management	80%
Technical Architecture	66%
Infrastructure and Operational Readiness	24%

Please let me know if you have any questions or concerns. Have a great weekend.

Thank you,

[redacted]

CGI [redacted], PMP | Manager | CGI Federal – Health & Compliance

office [redacted] | [redacted] | 593 Herndon Parkway, Herndon, VA [redacted]

We cannot solve our problems with the same thinking we used when we created them. – Albert Einstein

CONFIDENTIALITY NOTICE: Proprietary/Confidential Information belonging to CGI Group Inc. and its affiliates may be contained in this message. If you are not a recipient indicated or intended in this message (or responsible for delivery of this message to such person), or you think for any reason that this message may have been addressed to you in error, you may not use or copy or deliver this message to anyone else. In such case, you should destroy this message and are asked to notify the sender by reply e-mail.

Please consider the environment before printing this email or its attachments.

Exhibit 5

Email from CGI to HHS and CMS officials. Aug. 24, 2013.

From: [redacted]]
Sent: Saturday, August 24, 2013 11:32 AM
To: Thompson, Tyrone (CMS/OIS) (tyrone.thompson2@cms.hhs.gov)
CC: Oh, Mark U. (CMS/OIS) (mark.oh@cms.hhs.gov); [redacted] (CGI Federal); [redacted]. [redacted] (CGI Federal); 'lbjones@mitre.org' (lbjones@mitre.org); Van, Hung B. (CMS/OIS) (Hung.Van@cms.hhs.gov); Jenkins, Michelle L. (CMS/OIS) (Michelle.Jenkins@cms.hhs.gov); [redacted] (CGI Federal); Webber, JoAnn (CMS/OIS) (JoAnn.Webber@cms.hhs.gov) (JoAnn.Webber@cms.hhs.gov); Henry, Galina (CMS/OIS) (Galina.Henry@cms.hhs.gov) (Galina.Henry@cms.hhs.gov); Bing Chao (Bing.Chao@cms.hhs.gov) (Bing.Chao@cms.hhs.gov); Mageras, Nicholas [USA] (mageras_nicholas@bah.com) (mageras_nicholas@bah.com); [redacted] (CGI Federal); stuart.grant@genovatech.com; FFE CCIIO Communications; [redacted] (CGI Federal); [redacted] (CGI Federal); [redacted] (CGI Federal); [redacted] (CGI Federal); Alvarez, Carlos (CMS/OIS); Dunick, Walter T. (CMS/OIS); Lazenby, Daniel (CMS/OIS); polise_anthony@bah.com; Paul.Donohoe@cms.hhs.gov; Lewis, Angela [USA] (Lewis_Angela@bah.com); Grace.Suk@cms.hhs.gov; [redacted] (CGI Federal); [redacted] (CGI Federal); Mohs, Dean F. (CMS/CCIIO); Schneer, Seth H. (CMS/CCIIO); Grace.Suk@cms.hhs.gov; Luan Nguyen (luan.nguyen@relis-llc.com); [redacted] (CGI Federal); Amos, Robert E. (CMS/OC) (Robert.Amos@cms.hhs.gov); Duve, Rebecca J. (CMS/CTR) (Rebecca.Duve@cms.hhs.gov); 'Hase, Jason' (Jason.Hase@noblis.org); Rowen, Stanley [USA]; Hoang, Teresa [USA]; colin.mcveigh@cms.hhs.gov [redacted] (CGI Federal); Couts, Todd (CMS/OIS) (Todd.Couts1@cms.hhs.gov) (Todd.Couts1@cms.hhs.gov); [redacted] (CGI Federal); [redacted] (CGI Federal)
Subject: RE: Updated FFM Integrated Schedule
Attachments: FFM_IMS.zip

Hi Tyron,

I just noticed I had sent the wrong file. Please the updated file for August 23th in the attachment. Thank you!

Name	% Complete
FFM	62%
Eligibility and Enrollment	65%
SHOP	35%
Plan Management	90%
Financial Management	26%
Technical Architecture	69%
Infrastructure and Operational Readiness	76%

Contains Sensitive and Proprietary Business Information -- Maintain as Confidential

Exhibit 6

TurningPoint. IV&V Assessment 11v2. Executive Summary. Aug. 30, 2013.

CENTERS FOR MEDICARE & MEDICAID SERVICES
Office of Information Services
7500 Security Boulevard
Baltimore, MD 21244-1850

Federal Marketplace Program System (FMPS) Independent Verification & Validation (IV&V) Assessment 11 Report

Version 2.0
30-Aug-2013

Prepared by:

TurningPoint
TurningPoint Global Solutions
Software Services Company™

Document Number: FEPSIVV-IAR-11
Contract Number: HHSM-500-2012-00008U

This report presents the results of the quick "mini" assessment performed by the Independent Verification & Validation (IV&V) contractor, TurningPoint Global Solutions, who was tasked by the Centers for Medicare and Medicaid Services (CMS) to provide monthly technical audits of the Federal Marketplace Program System (FMPS). The team focused on providing information that is helpful for the governance of CGI's 8/15 release, primarily the Eligibility & Enrollment (E&E) component. The following areas were covered: defect analysis, requirements analysis, static code analysis, developmental test coverage analyis and analysis of release management.

There are significant deficiencies and weaknesses in all aspects of the development of the Federally-Facilitiated Marketplace (FFM), especially Individual Application, Plan Compare and My Account. This report provides an overall overview, functional area overviews and drill-downs to detailed information.
Of note: Based on the way the build notes were captured, we were unable to verifably trace requirements to the build.

Please click on the links below to view the supporting details.

For the near-term, the IV&V team recommends:
1. The new development and deployment processes (e.g., jolts, paths) should be defined and adequately communicated to the development teams.
2. Develop and communicate across the program all major and minor changes in real-time. Use CALT to communicate!
3. Engage the IV&V team early and in all critical meetings.
4. Strengthen decision-making by establishing checkpoints with real quality criteria (e.g., checklists, sign-offs).
5. Develop stronger performance-based program objectives for the accountable organizations.
6. Develop a streamlined issue management process to support the Oct. 1 go-live.
7. Consider performing developmental and ACA testing in parallel to improve defect identification and resolution process.
8. Ensure that developmental test coverage is adequate for all paths (10/1 - 12/1).
9. Consider developing SLAs with quality objectives and enforce governance.

Legend: Red = High Risk, Yellow = Moderate Risk, Green = Low Risk

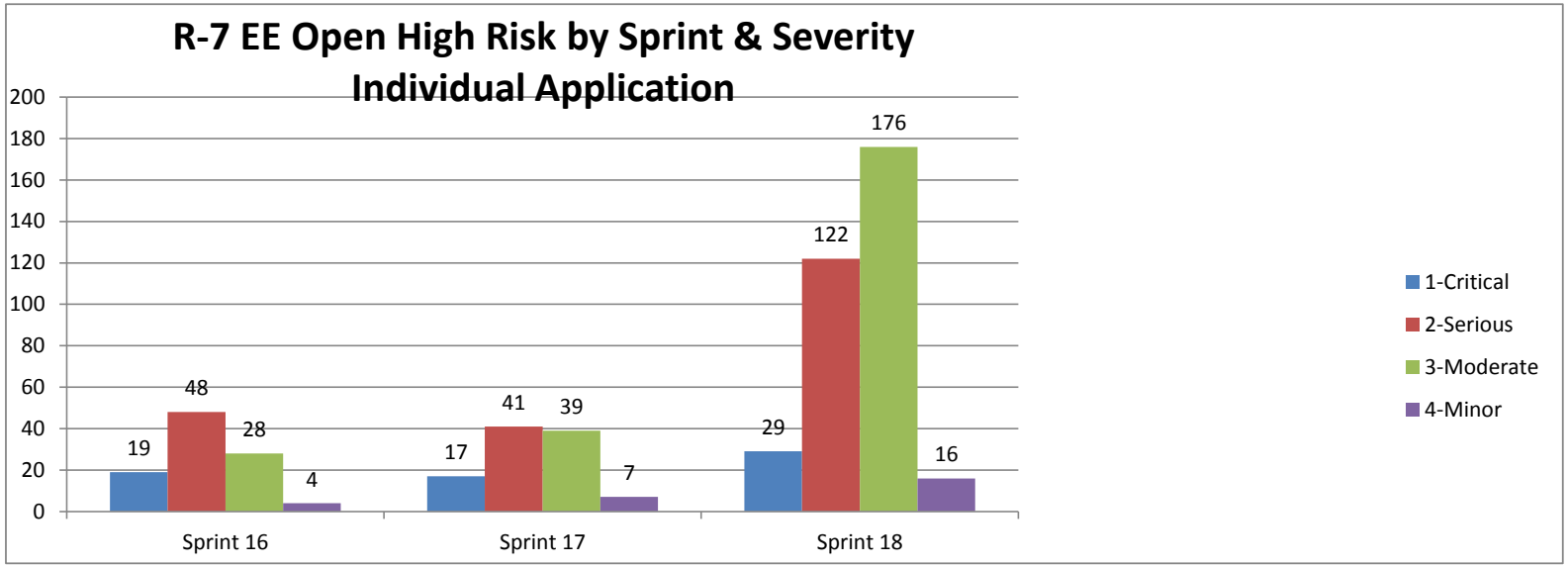
Release 7 CGI Documents for Enrollment & Eligibility	**Overall Risk Rating***	Analysis of Defects	Analysis of Requirements	Static Code Analysis	Analysis of Developmental Test Coverage	Analysis of Release Management
Direct Enrollment API	12.33	5.00	Not Reviewed	12.00	20.00	
E&E Federal Functions	5.00	Not Reviewed	Not Reviewed	Not Reviewed	5.00	
Call Center Integration	14.87	12.00	12.60	Not Reviewed	20.00	Overall E&E
Individual Application	19.55	25.00	21.20	12.00	20.00	Findings - not
Enrollment	13.77	Not Reviewed	10.20	11.11	20.00	evaluated by
Plan Compare	19.60	25.00	17.40	16.00	20.00	component
Eligibility Support Desktop	10.27	5.00	5.80	Not Reviewed	20.00	
My Account	17.80	25.00	16.40	12.00	Not Reviewed	

Release 7 CGI Documents for Plan Management	Static Code Analysis
Plan Management	12.93
Release 7 CGI Documents for Financial Management	
Financial Management	12.25

Defect Analysis
(as of August 26, 2013 Defect Report)

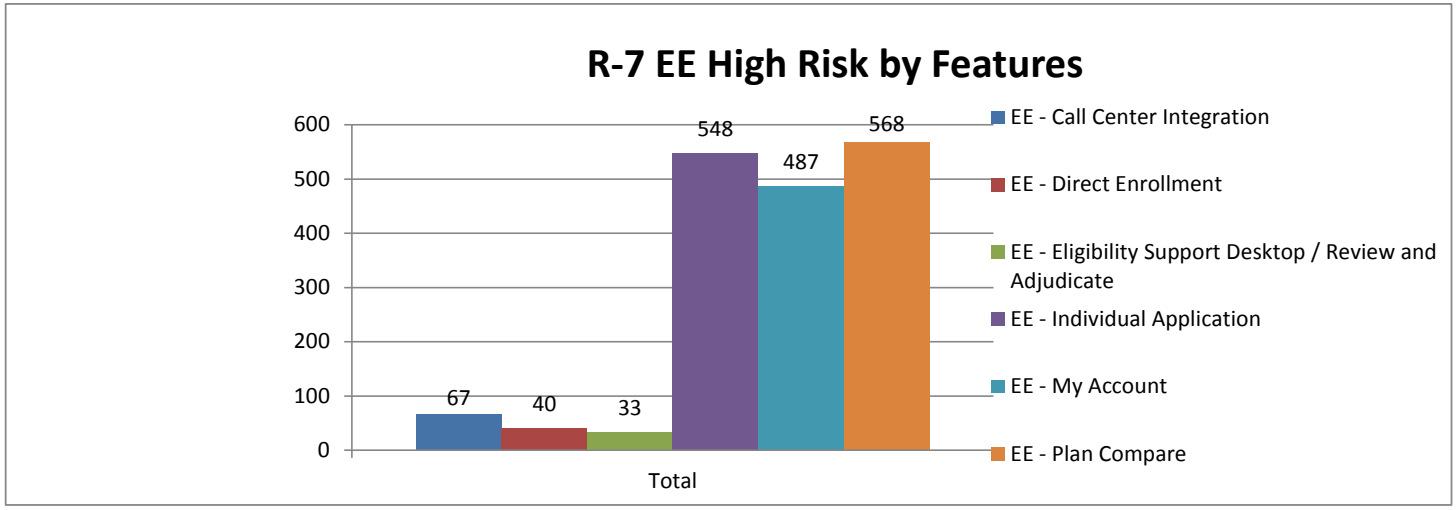
The following data was taken from August 26, 2013 HP Quality Center Extract (doc47977-Defects_in_FFE-Report_20130826_0900). According to the Agile methodology, defect resolution should decrease from one Sprint to another. In this case it increases.

CMS could have used story point measurements to predict the velocity for short-term and long-term indicators of risk to trigger preventive and corrective management actions.

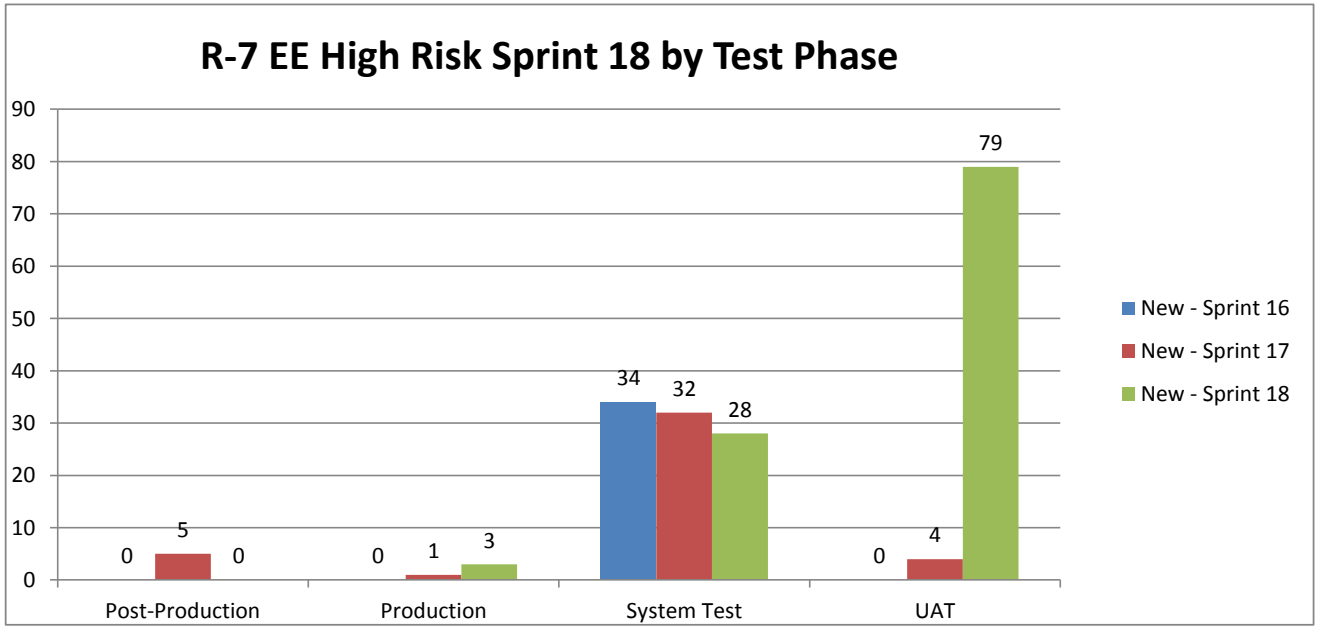


Defect Analysis
(as of August 26, 2013 Defect Report)

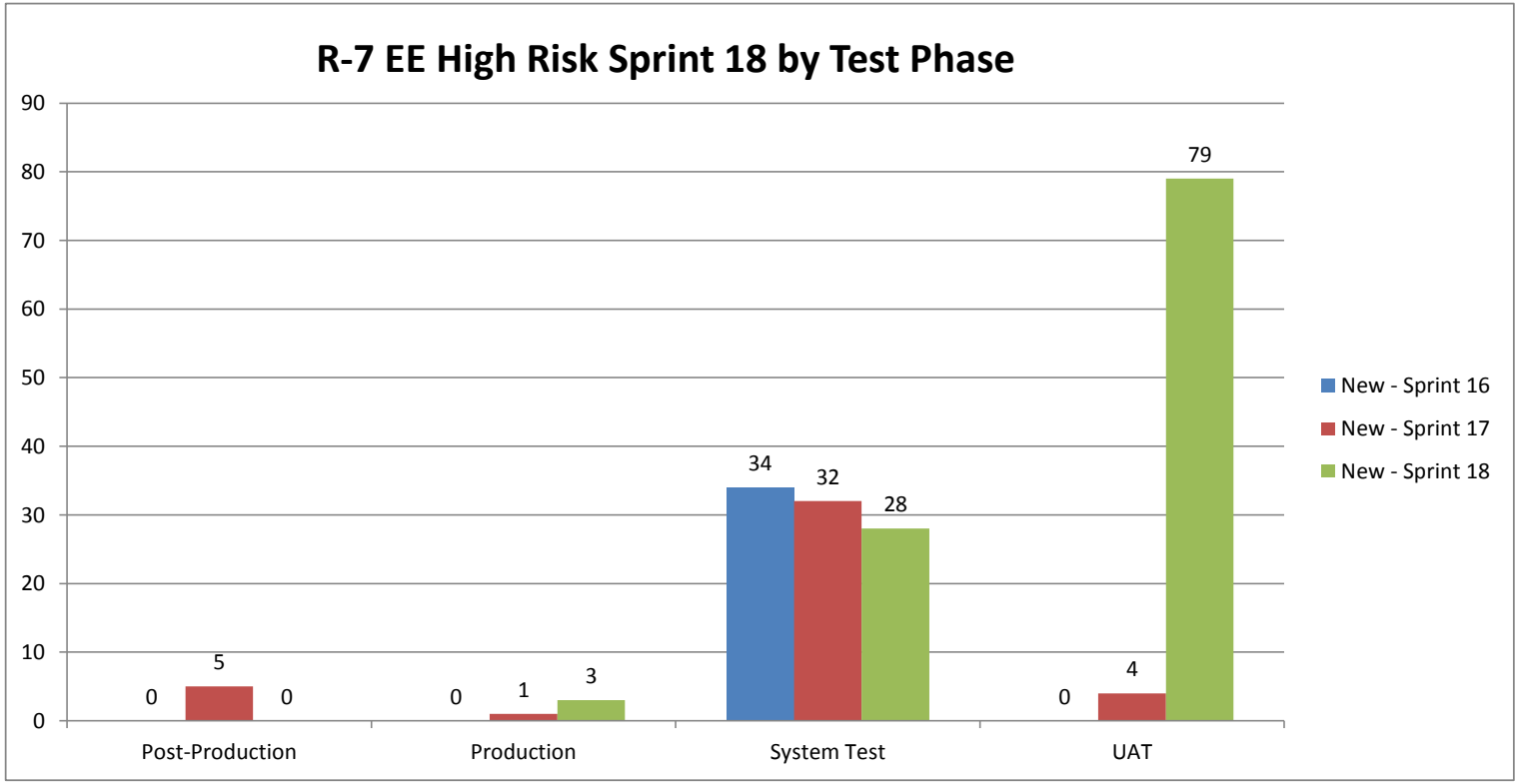
The highest number of defects is shown in Plan Compare (568), Individual Application(548) and My Account(487).



EE Individual Application has the highest number of defects in Sprint 18 (40%). Plan Compare has the second highest number of bugs (33%), and EE My Account has the third highest number of bugs (15%).

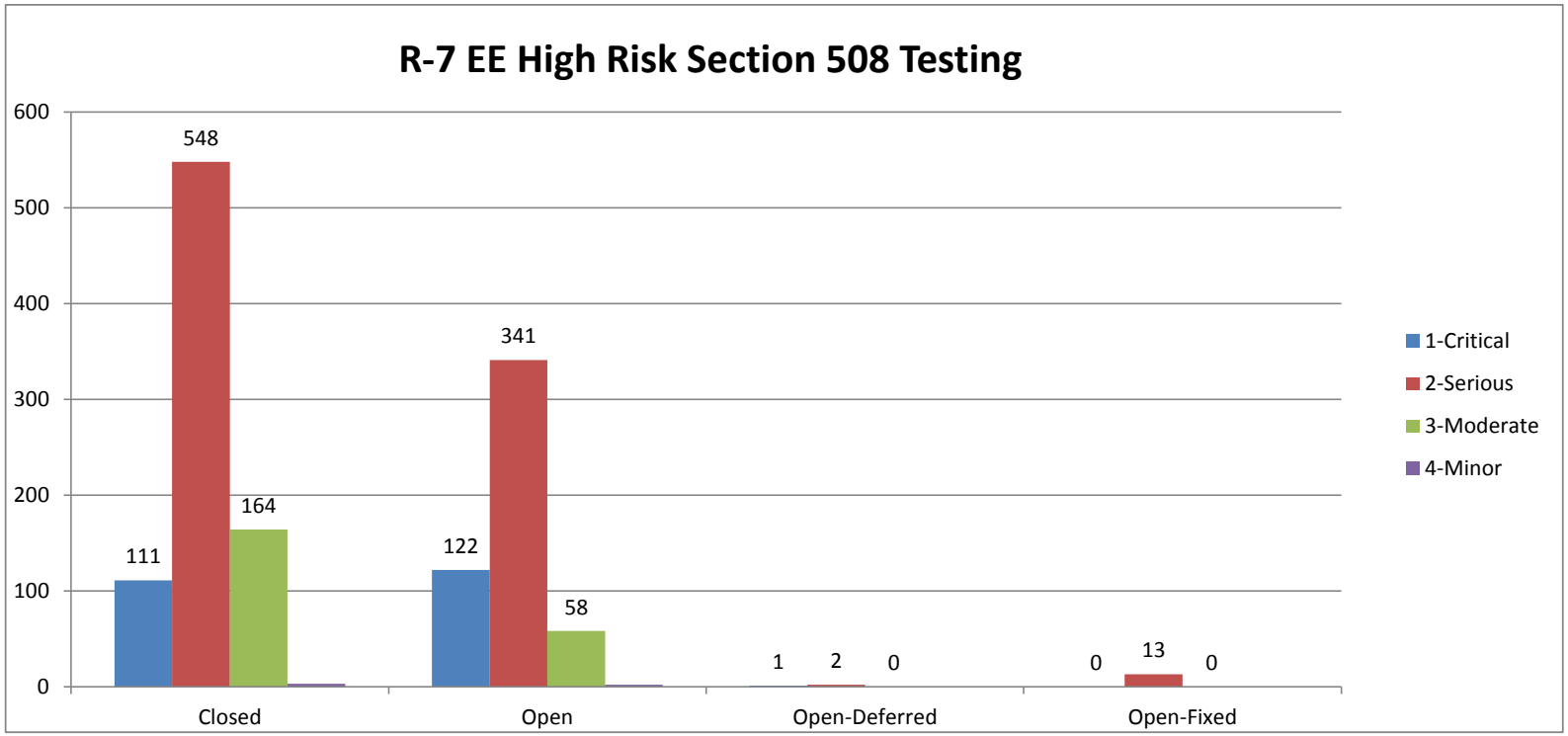


Number of new defects open for Sprint 18 in UAT is greater than for System Test. The opposite is what is expected.



Defect Analysis
(as of August 26, 2013 Defect Report)

Although a large number of defects have been closed, the high number of critical and serious defects that remain open for testing Section 508 needs to be closed prior to go live.



General Findings: Release Management

1. **Finding 1:** FMPS contractor current development practices focuses more on fixing a deployed system rather than building the final system. This doesn't follow an agile methodology to deliver quality code at the end of each Release.

   Recommendations:

   Agile Manifesto: Value 2: Working Software over Comprehensive Documentation

   A development team's focus should be on producing working products. On agile projects, the only way to measure whether you are truly done with a product requirement is to produce the working product feature associated with that requirement. For software products, working software means the software meets what we call the definition of done: at the very least, developed, tested, integrated, and documented. After all, the working product is the reason for the project.

2. **Finding 2:** There is no overarching consistent updated schedule or plan that addresses the content, development, and deployment of all planned FMPS services. As a result, it is difficult to determine the final version of the various services in terms of the functionality that will be delivered to the end users.
   Recommendation: Ensure all stakeholders provide a timely updates of their respective artifacts to ensure that relevant information is shared on a timely basis.

3. **Finding 3:** The lack of a clear system definition and detailed implementation plan prevents CMS from determining realistic cost estimates for future development, and presents a serious risk to CMS's ability to develop and deploy the final system

   Recommendation: Ensure an up to date implementation plan is in place. Also, monitor the execution of the plan on a frequent basis to prevent any risks that would jeopardize the project.

4. **Finding 4:** Testing continues to be hampered by the lack of clear requirements. That is, the system is developed based on general descriptions of functionality; they are not a by-product of detailed design stemming from well-defined user stories. This makes it difficult for the testers to plan and prepare test cases that completely test the implemented functionality.

5. **Finding 5:** Release documentation (Release Notes) not produced on time at the end of each build. The deployed system may not satisfy all its expected capabilities and problems may be missed during the formal testing of a build.

6. **Finding 6:** There is no unified calendar for complete visibility to development teams, release managers and operations teams with a consolidated view of all planned activities as well as infrastructure changes.

   Recommendation: By leveraging a unified calendar, the development and release teams are fully aware of the available windows for change, as well as the scheduled production down-times. This knowledge enables these teams to choose the appropriate time to request an infrastructure change. By linking approved development releases to existing operational maintenance windows, teams can avoid release delays and confusion during deployments

7. **Finding 7:** There is no evidence of a release checklist to help identify when the product is ready to be released:
   Recommendation: the release checklist should cover:
   a. The number of defects is at an acceptable level by CMS.
   b. All serious code violations are resolved before continuing development.
   c. Product performance and server loads are within acceptable margins
   d. Documentation is up to date, clear, complete and consistent
   e. Final sign off by CMS

Exhibit 7

TurningPoint. IVV Assessment 12. Senate Committee Staff Analysis. Oct. 23, 2013.

CENTERS FOR MEDICARE & MEDICAID SERVICES
Office of Information Services
7500 Security Boulevard
Baltimore, MD 21244-1850

Federal Marketplace Program System (FMPS) Independent Verification & Validation (IV&V) Assessment 12 Report

Version 2.0
23-Oct-2013

Prepared by:

Document Number: FEPSIVV-IAR-12
Contract Number: HHSM-500-2012-00008U

Risk Analysis Worksheet

Process Name	Finding ID	Evaluation Criteria	Evidence	Gap Description	Recommendation	Risk Probability	Risk Impact	Risk Score	Risk Level	Inputs Reviewed	COBIT Control ID
Ensure Risk Optimization	RSK001	1. The program is managing critical IT-related program risks effectively and efficiently. 2. IT-related risks are identified, analyzed, managed and reported.	A paper trail does not exist within CALT which captures meeting notes (participation by individuals -- triage team AND Risk Review Working Group, roles involved in the discussion, evaluation of new/existing risks/issues to the updated paths schedule) The Program calendar does not reflect the meeting frequency	A paper trail does not exist on CALT which captures meeting notes. It's not evident that risk/issue management meetings are regularly held by the RISK REVIEW WORKING GROUP to review new risks, close existing risks or provide coordinated updates.	Ensure meeting minutes capture summary discussion, identified risks, potential analysis, interdependencies related to the risk and proposed mitigations. Ensure satisfactory participation is represented at all meetings and a regular calendar invite is extended to all optional participants with sufficient notice.	4	3	12	**Moderate**	Risk Register - Project: CMS Federal Exchange Program Change and Risk Management Systems.	EDM03
Ensure Risk Optimization	RSK002	1. The program is managing critical IT-related program risks effectively and efficiently.	Risk updates - on average risks are 35 days older than their target close date. **Reviewed 51 risks with a target close date <= 9/13/2013.**	Risks/issues are not resolved timely. On average risks are 35 days older than the established Target Close Date on the Risk Register in CALT	Ensure risk estimates reflect all relevant information, topics, documents, meetings discussions and evaluation/analysis/mitigation participation includes appropriate SMEs to establish realistic closure dates.	5	4	20	**High**	Risk Register	EDM03
Ensure Risk Optimization	RSK003	IT-related program risks does not exceed risk appetite of the program	Minimum acceptable quality criteria doesn't exist for: requirements traceability to design documentation and user story completeness, development completeness, test/defect management, planned vs. actual test execution, change management effectiveness. Lack of enforcement of check points for code promotion. Lack of controls for CALT usage by contractors. Failure to develop and enforce corrective actions related to contractor poor performance, schedule slippage as it relates to risks	It's not evident the program has established acceptable risk tolerances that may impact the 10/1 GO LIVE.	Establish an appropriate level of risk acceptance for the 10/1 GO LIVE. Risk acceptance should be based on solution deliverable completeness, an evaluation of performance quality measures, solution completeness criteria, solution correctness criteria, test/defect management quality and performance goals with appropriate metrics that may bear on risk to the program.	5	5	25	**High**	Risk Management Plan	APO12
Manage Risk	RSK004	Risks are vetted by the Risk Triage Team before placement on the Risk Register; Risk Review Working Group (RRWG)	There isn't a paper trail which provides evidence regular meetings take place to validate identified risks. Risks discussion are not included as regular discussion topics on meeting agendas IV&V attends as an observer.	The process used by the Risk Triage Team to vett risks prior to placement on the Risk Register in the CALT Tracker is not transparent.	Provide greater transparency for how risks are being vetted. Identify the activities, roles, inputs etc… to ensure risks are given the highest attention and analysis. This will help to standardize the vetting process and help to establish realistic planned closure dates.	4	3	12	**Moderate**	CMS FFE Risk Management Plan v 1 2 Final Draft; Risk Management Workflow	APO12
Manage Risk	RSK005	Identify risks to cost, schedule, and technical performance early and continuously, such that control in any of these dimensions is not lost or the consequences of them are well understood.	Regular meetings IV&V participates in don't include discussion of new risks discovered in the meeting or updates to existing risks related to the meeting topic. Integration Meeting, Daily Production Meeting, FEPS Test Status Meeting, Canonical Data Model Meeting etc…	It's not clear how risks or issues are captured in regular and adhoc meetings.	Ensure a standard agenda is used for all meetings. It should reflect risks as a re-occurring topic. This will ensure that risks are given special attention at every level of program communication. The goal is to standardize the approach used for identification and review prior to submission.	4	4	16	**High**	Meetings Attended: List the meetings Risk Management Workflow Risk Management Plan	APO12
Manage Programs and Projects	RSK006	The program and project activities are executed according to the plans.	Use summary evidence captured in report	It's not evident the program implements IV&V recommendations in a timely way to improve program execution activities and minimize quality/completeness deficiencies.	Provide a mechanism to ensure directed actions from CMS Program Executive Leadership to FEPs contractors and Program federal staff are addressed and can be supported by objective evidence in plans, actions, technical documents, development code, requirements, CALT update activities etc..	4	4	16	**High**		BAI01

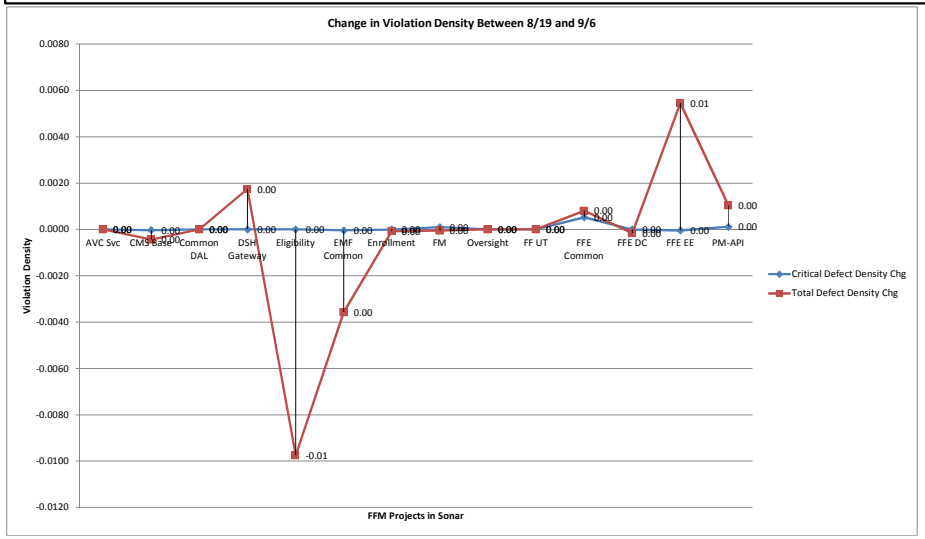
High	Moderate	Low

Introduction

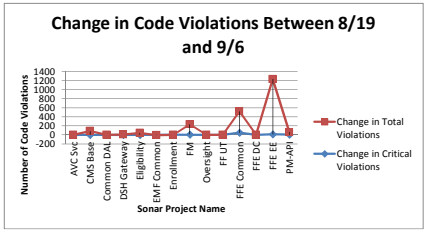
For this report, the IV&V team reviewed all of the code checked into SVN on 8/19/13 and 9/6/13. The graph below shows that there is a proportional number of violations in the new lines of code from IV&V Assessment #11. The yellow indicates areas of change from the previous assessment. There is no evidence that code violations are being given attention.

Project	Short Name	Lines of Code	Crit Defect Density	Total Defect Density	Lines of Code	Crit Defect Density	Total Defect Density	Critical Defect Density Chg	Total Defect Density Chg	Classes	Classes	SD-14, Number of Critical Violations	SD-14, Number of Critical Violations	SD-14, Total Number of Violations	SD-14, Total Number of Violations	SD-13, Comments %	SD-13, Comments %	Dulications %	Dulications %	Complexity (Number/Method)	Complexity (Number/Method)	Complexity (Number/Class)
Date		**8/19/2013**	**8/19/2013**	**8/19/2013**	**9/6/2013**	**9/6/2013**	**9/6/2013**			**8/19/2013**	**9/6/2013**	**8/19/2013**	**9/6/2013**	**8/19/2013**	**9/6/2013**	**8/19/2013**	**9/6/2013**	**8/19/2013**	**9/6/2013**	**8/19/2013**	**9/6/2013**	**8/19/2013**
AVC SOAP WS Service (tags/PRIME7_081913_01/PRIME_090613_01 version 6.2)	AVC Svc	1030	0.0039	0.0155	1030	0.0039	0.0155	0.00000	0.00000	6	6	4	4	16	16	8.2	8.2	55.5	55.5	10.5	10.5	29.7
CMS Base Project (tags/PRIME7_081913_01/PRIME_090613_01 version 7.0)	CMS Base	64406	0.0017	0.0600	66211	0.0016	0.0595	-0.00003	-0.00044	871	895	108	109	3862	3941	12.7	12.7	7.5	7.7	3.3	3.3	13.1
Common DAL (tags/PRIME7_081913_01/PRIME_090613_01 version 1.2)	Common DAL	904	0.0022	0.0940	904	0.0022	0.0940	0.00000	0.00000	18	18	2	2	85	85	12.8	12.8	0	0	3.4	3.4	9.6
DSH Gateway Project (tags/PRIME7_082113_02/PRIME_090613_01 version 7.0)	DSH Gateway	1990	0.0000	0.0749	2010	0.0000	0.0766	0.00000	0.00174	36	36	0	0	149	154	26	26.2	4.4	5.2	4.2	4.2	6.2
Eligibility (tags/PRIME7_081913_01/PRIME_090613_01 version 7.0)	Eligibility	773	0.0000	0.0530	1848	0.0000	0.0433	0.00000	-0.00975	10	16	0	0	41	80	16.5	11.7	13	16.2	2.8	3.3	14.5
EMF Common (tags/PRIME7_081913_01/PRIME_090613_01 version 7.0)	EMF Common	2690	0.0030	0.0807	2724	0.0029	0.0771	-0.00004	-0.00358	47	49	8	8	217	210	16.8	16.7	1	1	2.7	2.7	9.9
Enrollment (tags/PRIME7_081913_01/PRIME_090613_01 version 7.0)	Enrollment	1335	0.0007	0.0914	1347	0.0007	0.0913	-0.00001	-0.00007	11	11	1	1	122	123	10.2	10.1	8.2	8.1	4.4	4.5	23.4
FF FM Project (tags/PRIME7_081913_01/PRIME_090613_01 version 7.0)	FM	41698	0.0010	0.0796	44542	0.0011	0.0796	0.00009	-0.00006	599	635	41	48	3321	3545	15.9	16.2	8.9	9	3.6	3.6	12.4
FF Oversight URR Project (tags/PRIME7_081913_01/PRIME_090613_01)	Oversight	23888	0.0008	0.0580	23888	0.0008	0.0580	0.00000	0.00000	267	267	19	19	1386	1386	8.2	8.2	10.2	10.2	5.3	5.3	14.6
FF UT Project (tags/PRIME7_081913_01/PRIME_090613_01 Version 6.2)	FF UT	2200	0.0005	0.0495	2200	0.0005	0.0495	0.00000	0.00000	24	24	1	1	109	109	6.1	7.3	6.1	6.1	5.4	5.4	15
FFE Common Project (tags/PRIME7_080313_01/PRIME_090213_03 Version 7.0)	FFE Common	55393	0.0020	0.0578	62644	0.0025	0.0586	0.00052	0.00080	464	526	110	157	3199	3668	23.1	22.4	9.4	8.8	7.1	6.9	24.1
FFE DC Project (tags/PRIME7_082113_02/PRIME_090613_01 Version 6.2)	FFE DC	31163	0.0028	0.0661	31237	0.0028	0.0660	-0.00001	-0.00016	290	291	86	86	2061	2061	10.4	10.3	9.3	9.4	6.2	6.2	23.6
FFE EE Project (tags/PRIME7_082113_02/PRIME_090913_01 version 7.0)	FFE EE	69573	0.0007	0.0348	90496	0.0007	0.0402	-0.00004	0.00545	534	665	50	61	2419	3640	16.3	16.9	8.3	9.8	5.8	5.9	26.9
PM-API (tags/PRIME7_082113_02/PRIME_090613_01 version 7.0)	PM-API	23123	0.0032	0.0667	23567	0.0033	0.0677	0.00011	0.00103	281	284	74	78	1542	1596	11.4	11.2	15.2	15.3	3.8	3.8	14

The following graph depicts the change in code violation density between 8/19/13 and 9/6/13 (as defects from testing are being corrected). A negative number indicates decreased code violation density and a positive number indicates increased code violation density. Overall, there has been little change in defect density. For the Eligibility Sonar project, there was decreased *Total Code Violation Density* of -.01. However, there were only 1,848 lines of code present in the Eligibility Sonar project on 9/6/13. This translates to approximately 18 fewer code violations than were present at 8/19. In actuality, there were a total of 41 Total Code Violations on 8/18/13 for 773 lines of code and now there are 80 Total Code Violations for 1,848 lines of code. On the other hand, for the FFE EE Sonar Project, which showed an increase in Total Density of .00545 with 90,496 lines of code, representing an increase of 1221 violations.



Short Name	Change in Critical Violations	Change in Total Violations
AVC Svc	0	0
CMS Base	1	79
Common DAL	0	0
DSH Gateway	0	5
Eligibility	0	39
EMF Common	0	-7
Enrollment	0	1
FM	7	224
Oversight	0	0
FF UT	0	0
FFE Common	47	469
FFE DC	0	0
FFE EE	11	1221
PM-API	4	54



Project	Complexity (Number/Class)	Rules compliance %	Rules compliance %	Package Tangle Index (SD-14,Coupling) %	Package Tangle Index (SD-14,Coupling) %	Unreviewed Violations	Unreviewed Violations	SD-19, unit test success %	SD-19, unit test success %	SD-19, Code Coverage of Testing %	SD-19, Code Coverage of Testing %	SD-19, Code Coverage /lines %	SD-19, Code Coverage /lines %	SD-19, Code Coverage /branches %	SD-19, Code Coverage /branches %
Date	**9/6/2013**	**8/19/2013**	**9/6/2013**	**8/19/2013**	**9/6/2013**	**8/19/2013**	**9/6/2013**	**8/19/2013**	**9/6/2013**	**8/19/2013**	**9/6/2013**	**8/19/2013**	**9/6/2013**	**8/19/2013**	**9/6/2013**
AVC SOAP WS Service (tags/PRIME7_081913_01/PRIME_090613_01 version 6.2)	29.7	94.6	94.6	0.0	0.0	16	16	0	0	0	0	0	0	0	0
CMS Base Project (tags/PRIME7_081913_01/PRIME_090613_01 version 7.0)	13.1	84.5	84.7	5.5	5.7	3862	3941	100	98.9	14.5	16.4	14.5	16.3	14.3	16.6
Common DAL (tags/PRIME7_081913_01/PRIME_090613_01 version 1.2)	9.6	73	73	0.0	0.0	85	85	0	0	0	0	0	0	0	0
DSH Gateway Project (tags/PRIME7_082113_02/PRIME_090613_01 version 7.0)	6.2	77.6	77.7	0.0	0.0	149	154	100	100	0	0	0	0	0	0
Eligibility (tags/PRIME7_081913_01/PRIME_090613_01 version 7.0)	19.9	87.8	90.4	0.0	0.0	41	80	100	100	0	0	0	0	0	0
EMF Common (tags/PRIME7_081913_01/PRIME_090613_01 version 7.0)	9.6	78.2	78.5	0.0	0.0	217	210	100	100	34.8	34.5	37.7	37.4	21.9	21.9
Enrollment (tags/PRIME7_081913_01/PRIME_090613_01 version 7.0)	23.9	83.7	83.6	0.0	0.0	122	123	0	0	0	0	0	0	0	0
FF FM Project (tags/PRIME7_081913_01/PRIME_090613_01 version 7.0)	12.5	81	80.9	5.2	4.9	3321	3545	100	94.1	0.3	0.3	0.4	0.4	0.1	0.2
FF Oversight URR Project (tags/PRIME7_081913_01/PRIME_090613_01)	14.6	85.7	85.7	0.0	0.0	1386	1386	100	100	3.5	3.5	3	3	5	5
FF UT Project (tags/PRIME7_081913_01/PRIME_090613_01 Version 6.2)	15	87.1	87.1	0.0	0.0	109	109	0	0	0	0	0	0	0	0
FFE Common Project (tags/PRIME7_080313_01/PRIME_090213_03 Version 7.0)	23.7	89.3	89.3	11.1	9.2	3199	3668	100	100	4.3	2.4	4.9	2.1	3.1	3
FFE DC Project (tags/PRIME7_082113_02/PRIME_090613_01 Version 6.2)	23.6	82.9	82.9	1.0	1.0	2061	2061	100	100	7.7	7.7	6.9	6.9	9.2	9.2
FFE EE Project (tags/PRIME7_082113_02/PRIME_090913_01 version 7.0)	28.2	92.4	90.6	10.2	14.4	2419	3640	100	100	0.1	0.2	0.1	0.2	0	0.1
PM-API (tags/PRIME7_082113_02/PRIME_090613_01 version 7.0)	14.1	83	82.8	0.0	0.0	1542	1596	90.5	90.5	1.4	1.3	1.5	1.5	0.9	0.9

Introduction to Communication

Communication has been identified as one of the single biggest reasons for project success or failure. Effective communication within the project teams, and between the management organization and external stakeholders, is essential. Openness in communication is a gateway to teamwork and high performance. If the purpose of a particular type of communication is to convey large volumes of information or information to very large audiences, an organization should use a form of "pull communication," such as websites*. For the FMPS program, the mandated tool for this is CALT. If the purpose of a type of communication is to ensure that information is distributed, then the organization should use a form of "push communication," such as milestone review presentations, memos, reports, and emails. If the purpose of a type of communication is to ensure a common understanding and to have a multidirectional exchange of information, then a meeting should be used. If an interactive exchange of information is desired, then it is important to provide an agenda and to perform a roll call to ensure each organization is represented.

For this report, the IV&V team only reviewed a sampling of the communication taking place during interactive information exchange meetings, i.e., no brainstorming or decision making meetings were reviewed.

Gaps:

COM001 - No risks or issues were captured during the meetings that were sampled (PMBoK).
COM002 - Current action items are documented; however, there is no evidence that the action items are tracked to closure on the FMPS Morning Production, Touch Bases and Testing calls.
COM003 - There are continuing problems with required contractor representatives not being present in Morning Production, FMPS Touch Bases and Testing Status.
COM004 - Information is only provided by email if it is requested. There does not appear to be proactive planning for the distribution of information.

Recommendations:

COM001 - If the type of communication selected is a meeting, an information exchange is expected. Thus, it is important to perform a roll call prior to the start of the meeting to ensure that every organization is represented so that a complete exchange of information takes place.
COM002 - Formalize the communications from the current way of informally communicating through emails and ad hoc meetings.
COM003 - Provide updates to action items identified in previous meetings.
COM004 - Provide meeting and status information in CALT, and enforce governance over CALT for integrated and unified communication capabilities.

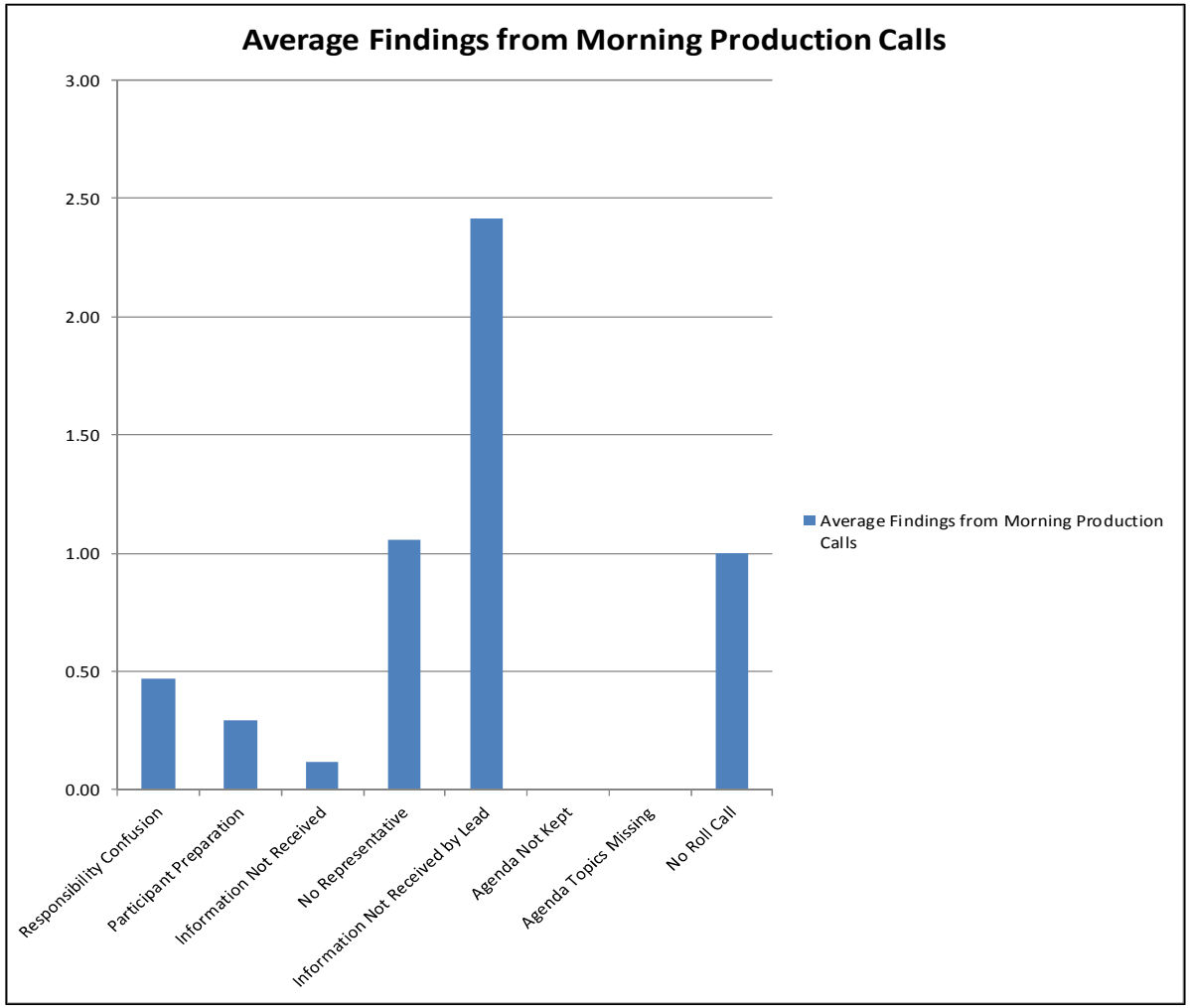
* Project Management Body of Knowledge, fifth edition, 2013.

The ***Daily Morning Production*** calls data shows the following:

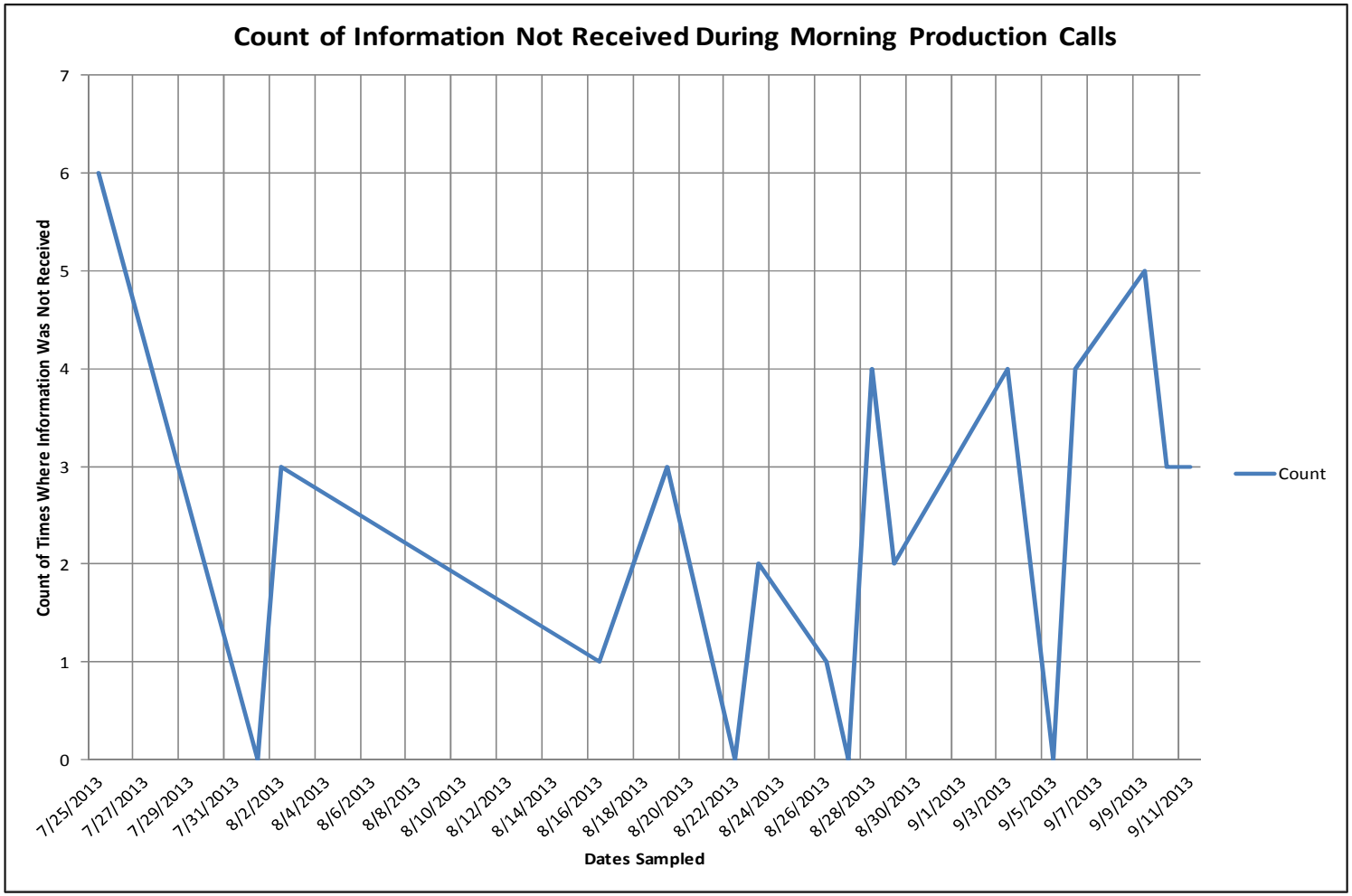
1. There is no evidence of an agenda in use.
2. On average, there is a considerable amount of information that the XOC Manager should be receiving from contractors, but contractors are not providing this information, e.g. statusing emails, Root Cause Analyses (RCAs), Change Requests (CRs), and Remedy tickets.
3. On average, at least one contractor organizational representative did not attend when they should have attended.
4. No roll call is performed.
5. Risks are not collected for the program's risk register.

Other items noted in the ***Daily Morning Production*** calls are: inconsistent sharing of information, detailed information is only emailed to specific people who ask for it and there is an inconsistent structure to the meeting.
The labels on the x-axis are based on findings related to PMBoK or CobIT:

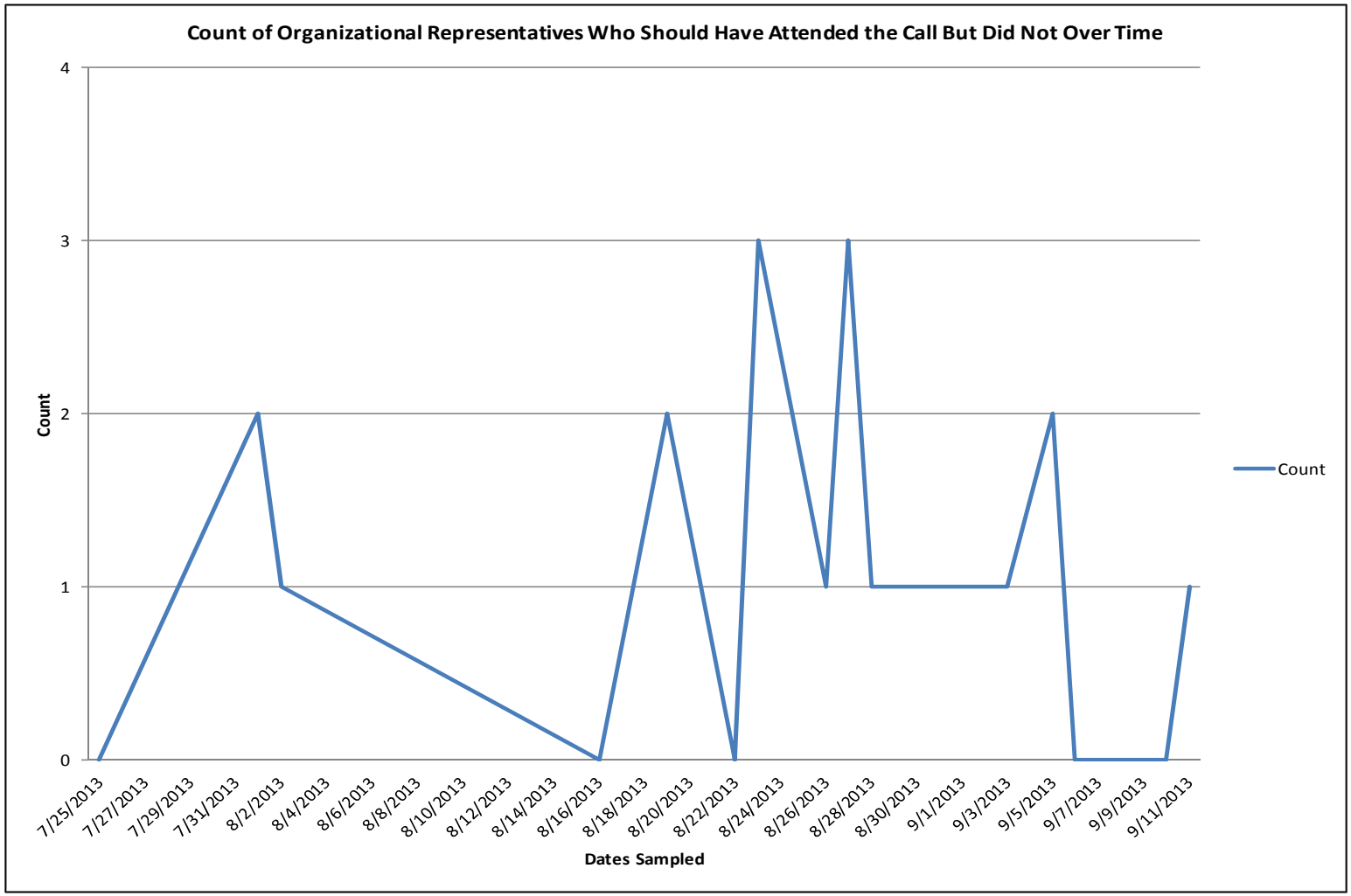
- Participant role/responsibility confusion: "I did not know I was supposed to do this or this was going to happen." (APO01-BP2)
- Participant not prepared with expected information. (APO01-BP2) A stakeholder who should have been getting information, had to request copy / email. (APO01-BP2)
- No required representative attended from organization. (APO01-BP2)
- Lead requested information that should have already been provided. (APO01-BP2)
- Agenda not maintained or greater than three tangents. (PMBok) Left out topics for discussion when there is an agenda. (PMBok)
- No roll call . (PMBok)



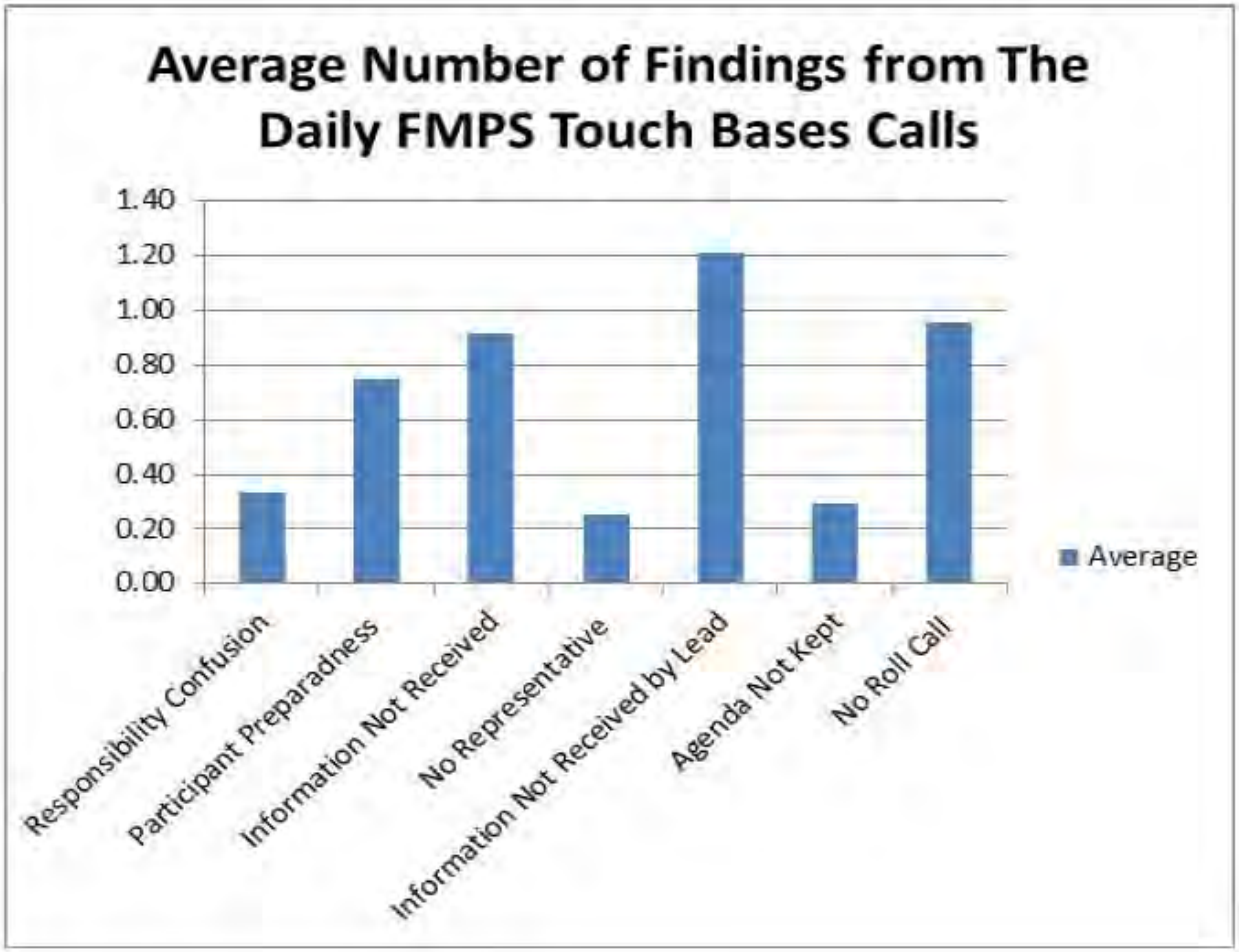
The following Daily Morning Production calls graph depicts no real change in the receipt of expected information over time. Contractor responsiveness has not improved.



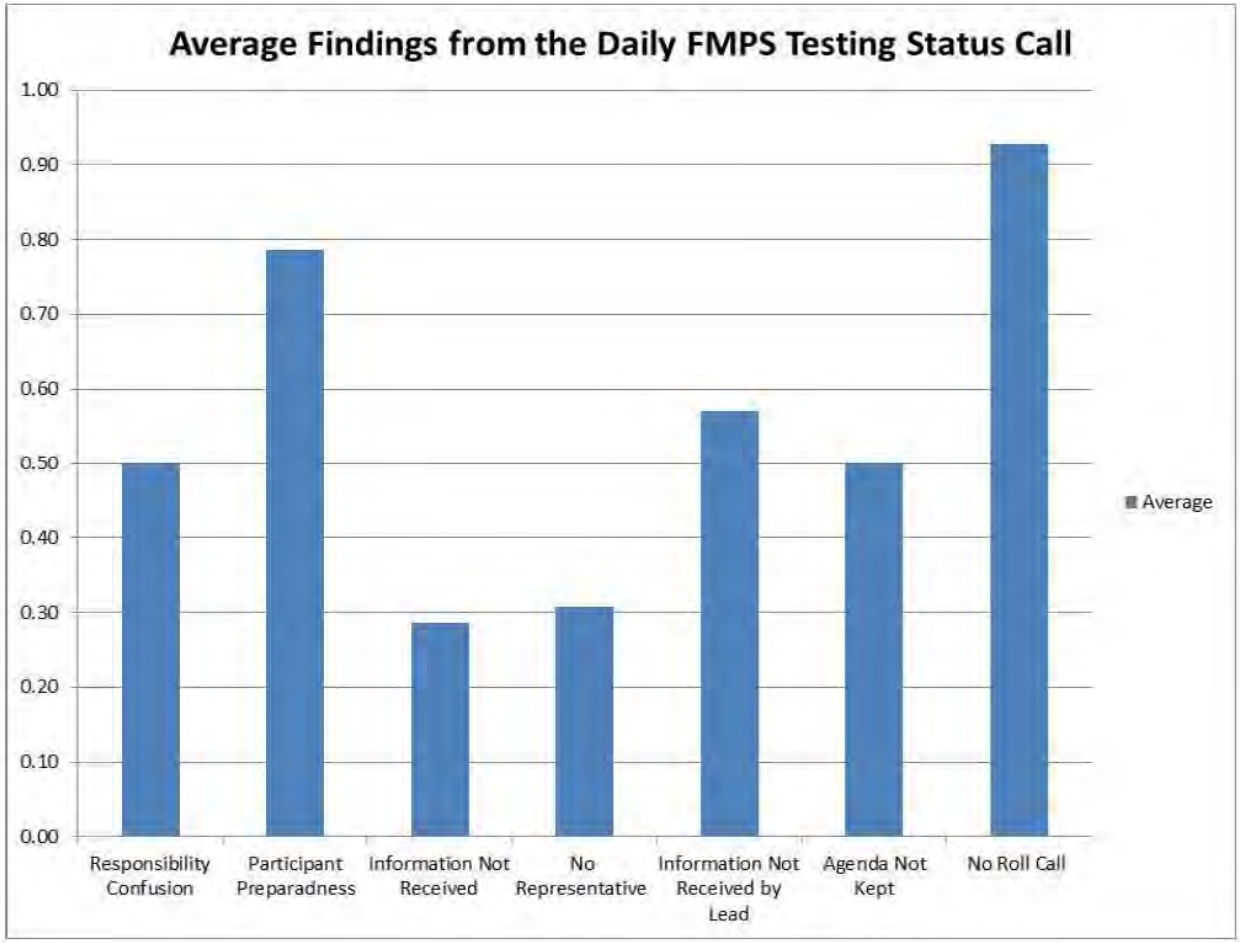
The following Daily Morning Production calls graph depicts no real change in the attendance of required organizational representative over the time sampled. Contractor responsiveness has not improved.



The following graph depicts an average of the count of each anomaly type in the Daily FMPS Touch Bases calls.



The following graph depicts an average of the count of each anomaly type in the Daily Testing Status calls.



Communication Control Objectives: APO11; APO01; APO02 (COBIT Controls)

1. Compliance with internal policies, processes and methodologies. (CALT is the key document repository for ALL FMPS development)
2. Communication activities support accurate and complete information exchange .
3. Ensure that critical and confidential information is withheld from those who should not have access to it.
4. Define and communicate quality requirements in all processes, procedures and the related program outcomes, including controls, ongoing monitoring, and the use of proven practices and standards in continuous improvement and efficiency efforts. - APO11
5. Clarify and maintain the governance of program IT mission and vision. Implement and maintain mechanisms and authorities to manage information in support of program governance objectives in line established program policies, guidelines and standards. - APO01
6. Provide a holistic view of the current business blueprint and IT environment, the future direction, and the initiatives required to implement the program into production. Leverage enterprise architecture building blocks and components, including externally provided services and related capabilities to enable nimble, reliable and efficient response to strategic objectives. - APO02
7. Align strategic IT plans with business blueprint objectives. Clearly communicate the objectives and associated accountabilities so they are understood by all, with the IT program strategic options identified, structured and integrated with the business plans. - APO02

Program Outcomes: APO01-O1, APO01-O2; APO11-O1; APO02-O5

1. Communication demonstrates an effective use of messaging channels .
2. Communication captures accurate and complete information which enables management to make effective and timely decisions.
3. Meetings formats, frequency and topics capture appropriate information to facilitate efficient resource participation and mitigate risks.
4. Policies are defined, determined to be effective and are maintained.
5. Everyone is aware of the policies and how they should be implemented.
6. Stakeholders are satisfied with the quality of solutions and services.

Inputs:

1. Communication threads (meeting agendas, meeting minutes)
2. Communication processes
3. Communication policies
4. Communication procedures
5. Program decks
6. Status Reports
7. Identified gaps in IT services
8. Improvement action plans and remediation's
9. Corrective actions
10. Stage-gate review results
11. Examples of good practice to be shared
12. Quality review benchmark results

COBIT Process Name:	COBIT Process ID:
Manage the IT Management Framework	APO01
Manage Quality	APO11
Ensure Governance Framework Setting and Maintenance	EDM01
Manage Strategy	APO02
COBIT Governance Practice:	**COBIT Best Practice ID:**
Direct the governance system - Inform leaders and obtain their support, buy-in and commitment. Guide the structures, processes and practices for the governance of IT in line with agreed-on governance design principles, decision-making models and authority levels. Define the information required for informed decision making.	EDM01-BP1
Establish roles and responsibilities. Establish, agree on and communicate roles and responsibilities of IT personnel, as well as other stakeholders with responsibilities for enterprise IT, that clearly reflect overall business needs and IT objectives and relevant personnel's authority, responsibilities and accountability.	APO01-BP2
Communicate the IT strategy and direction - Create awareness and understanding of the business and IT objectives and direction, as captured in the IT strategy, through communication to appropriate stakeholders and users throughout the enterprise.	APO02-BP6
Define and manage quality standards, practices and procedures - Identify and maintain requirements, standards, procedures and practices for key processes to guide the enterprise in meeting the intent of the agreed-on QMS. This should be in line with the IT control framework requirements. Consider certification for key processes, organization units, products or services.	APO11-BP2
Perform quality monitoring, control and reviews - Monitor the quality of processes and services on an ongoing basis as defined by the QMS. Define, plan and implement measurements to monitor customer satisfaction with quality as well as the value the QMS provides. The information gathered should be used by the process owner to improve quality.	APO11-BP4
Integrate quality management into solutions for development and service delivery - Incorporate relevant quality management practices into the definition, monitoring, reporting and ongoing management of solutions development and service offerings.	APO11-BP5
Maintain continuous improvement -Maintain and regularly communicate an overall quality plan that promotes continuous improvement. This should include the need for, and benefits of, continuous improvement. Collect and analyze data about the QMS, and improve its effectiveness. Correct non-conformities to prevent recurrence. Promote a culture of quality and continual improvement.	APO11-BP6
Review Activities:	
Verify that communication and reporting mechanisms provide those responsible for oversight and decision-making with appropriate information.	

This report presents the results of the quick "mini" assessment performed by the Independent Verification & Validation (IV&V) contractor, TurningPoint Global Solutions, who was tasked by the Centers for Medicare and Medicaid Services (CMS) to provide monthly technical audits of the Federal Marketplace Program System (FMPS). The team focused on providing information that is helpful for the governance of Release 7. The following areas were covered: communications analysis, risk analysis, defect/static code analysis, test analysis and analysis of release management.

There are significant deficiencies and weaknesses in all aspects of the development of the Federally-Facilitated Marketplace (FFM), especially in the controls related to communication effectiveness, stakeholder engagement, adherence to risk management plans and strategies, solution build quality and test management. This report provides an overall objective assessment of risks associated with the aforementioned controls. IV&V's examination of key artifacts, observations in standing regular meetings and review of activities/action items focused on the October 1 Go Live produced the following critical findings that should be addressed in the near term:

1. There are numerous critical and major code violations in the FFM code, impacting the maintainability of the code, and contributing to defects.
2. Code violation density is unchanged from prior IV&V assessments.
3. No evidence of analysis being performed to focus resources for defect management.
4. CGI defect data was missing key data attributes which would have improved the defect analysis.
5. The IV&V Team was unable to identify a mitigation strategy or contingency plan for open critical defects in the system at Go-Live.
6. The IV&V Team was unable to ascertain the CMS acceptance thresholds for the numbers of open defects at Go-Live.
7. There is no indication of quality controls around migration of the builds between test environments.
8. There is no evidence of separation of duties in promoting code between development, test and production environments.
9. There is minimal adherence to the CMS Risk Management Plan.
10. Evidence was shown that more than 47% of defects were attributed to "Coding Not Per Requirement/Design."

For the near term, the IV&V Team recommends:

1. Ensure the program is following the established risk management plan. Establish an appropriate level of risk acceptance to address the program's risk acceptance threshold.
2. Perform code reviews using the CMS provided Sonar tool before testing.
3. Analyze defects and focus resources on defect resolution prior to Go-Live.
4. Complete the implement action of the IQ Suite tool for defect management with all required fields populated as soon as possible.
5. Establish success criteria for testing as part of release management when software is moved to the next environment.
6. Publish release management controls to ensure policy adherence across the program.
7. Perform Root Cause Analysis (RCA) to identify why coding does not meet requirements/design.
8. Ensure separation of duties for promotion of code to successive environments.

.

Introduction to Risk

The IV&V team evaluated multiple risk management artifacts, risk management practices and meeting activities. Evaluation findings were compared to Control Objectives for Information Technology (COBIT) version 5 processes (Manage Risk, Ensure Risk Optimization and Manage Programs and Project). Evidence captured provided IV&V a basis to form an objective opinion of the program's quality and effectiveness of risk management processes and risk tolerance associated with the October 1 Go-Live. All gaps and associated recommendations should be addressed immediately by Program Executive leadership prior to 10-1's GO-LIVE. In addition, Program Executive leadership should establish a risk appetite prior to the 10-1 GO-LIVE and immediately implement corrective measures to ensure greater transparency related to risk identification, risk validation, management and closure. Please refer to Tab: Appendix Risk Details for detailed risk information.

Gaps:

RSK001 - A paper trail does not exist within CALT which captures meeting notes. It's not evident that risk/issue management meetings are regularly held by the RISK REVIEW WORKING GROUP to review new risks, close existing risks or provide coordinated update.

RSK002 - Risks/issues are not resolved timely. On average risks are 35 days older than the established Target Close Date on the Risk Register in CALT .

RSK003 - It's not evident the program has established acceptable risk tolerances that may impact the 10/1 GO LIVE.

RSK004 - The process used by the Risk Triage Team to vett risks prior to placement on the Risk Register in the CALT Tracker is not transparent.

RSK005 - It's not clear how risks or issues are captured in regular and adhoc meetings.

RSK006 - It's not evident the program implements IV&V recommendations in a timely way to improve program execution activities and minimize quality/completeness deficiency.

Recommendations:

RSK001 Ensure meeting minutes capture the meeting summary discussion, identified risks, potential analysis, interdependencies related to the risk and proposed mitigations. Ensure satisfactory participation is represented at all meetings and a regular calendar invite is extended to all optional participants with sufficient notice to attend the meeting.

RSK002 Ensure risk estimates reflect all relevant information, topics, documents, meeting discussions and risk evaluation, risk analysis and participation includes appropriate SMEs to establish realistic closure dates.

RSK003 Establish an appropriate level of risk acceptance for the 10/1 GO LIVE. Risk acceptance should be based on solution deliverable completeness, an evaluation of performance quality measures, solution completeness criteria, solution correctness criteria, test/defect management quality and performance goals with appropriate metrics that may bear on risk to the program.

RSK004 Provide greater transparency for how risks are being vetted. Identify the activities, roles, inputs etc… to ensure risks are given the highest attention and analysis. This will help to standardize the vetting process and help to establish realistic planned closure dates.

RSK005 - Ensure a standard agenda is used for all meetings. It should reflect risks as a re-occurring topic. This will ensure that risks are given special attention at every level of program communication. The goal is to standardize the approach used for identification and review prior to submission.

RSK006 - Provide a mechanism to ensure directed actions from CMS Program Executive Leadership to FMPs contractors and Program federal staff are addressed and can be supported by objective evidence in plans, actions, technical documents, development code, requirements, CALT update activities etc..

Risk Management Control Objectives: APO12; EDM03; BAI01 (COBIT)

1. Establish clarity of business impact of risks to IT objectives and resources.
2. Ensure that the impact of IT risks to the FEPs program is identified and managed and the potential for compliance failures is minimized.
3. Continually identify, assess and reduce IT-related risk within levels of tolerance set by program executive management. - APO12
4. Ensure that the program's risk appetite and tolerance is understood, articulated and communicated, and that risk to program value related to program planning and execution is identified and managed.-EDM03
5. Manages all aspects of the project in alignment with the program's developing and implementation strategy in a coordinated way. Initiates, plans, controls, and executes the project, and closes each sprint or major delivery phase with a post-implementation review.- BAI01
6. Realize program benefits and reduce the risk of unexpected delays, costs and value erosion by improving communication to and involvement of program stakeholders and end users, ensuring the value and quality of program/project deliverables, and maximizing their contribution to the services portfolio.- BAI01

Program Outcomes: APO12-01 - APO12-04; EDM03-O1 - EDM03-O3; BAI01-O1; BAI01-O2; BAI01-O3; BAI01-O4; BAI01-O5

1. Risk thresholds are defined, communicated and key IT-related risks are known.
2. The program is managing critical IT-related program risks effectively and efficiently.
3. IT-related risks are identified, analyzed, managed and reported.
4. A current and complete risk profile exists.
5. All significant risk management actions are managed and under control.
6. Risk management actions are implemented effectively.
7. Risk thresholds are defined and communicated and key IT-related program risks are known.
8. IT-related program risks does not exceed risk appetite of the program.
9. Relevant stakeholders are engaged in the programs and projects.
10. The scope and outcomes of programs and projects are viable and aligned with objectives.
11. Program and project plans are likely to achieve the expected outcomes.
12. The program and project activities are executed according to the plans.
13. There are sufficient program and project resources to perform activities according to the plans.

Inputs:

1. Program risk management principles
2. Emerging risk issues and factors - APO12-WP3
3. Enterprise risk management profiles and mitigation plans
4. Risk analysis and risk profile reports for stakeholders - APO12-WP9
5. Risk analysis results - APO12-WP6
6. Opportunities for acceptance of greater risk - APO12-WP11
7. Project risk management plan - BAI01-WP21
8. Project risk assessment results - BAI01-WP22
9. Project risk register - BAI01-WP23
10. Approved risk tolerance levels - EDM03-WP2
11. Identified contractor delivery risk - APO10-WP7
12. Remedial actions to address risk management deviations - EDM03-WP7
13. IT risk scenarios - APO12-WP5
14. Project proposals for reducing risk - APO12-WP12

COBIT Process Name:	COBIT Process ID:	Associated Gaps
Manage Risk	APO12	RSK004, RSK0045
Ensure Risk Optimization	EDM03	RSK001, RSK002, RSK003
Manage Programs and Projects	BAI01	RSK006

COBIT Governance Practice:	COBIT Best Practice ID:
Evaluate risk management - Continually examine and make judgment on the effect of risk on the current and future use of IT in the program. Consider whether the program's risk appetite is appropriate and that risk to program value related to the use of IT is identified and managed.	EDM03-BP1

Review Activities:	
1. Determine the level of IT-related risk that the program is willing to take to meet its objectives (risk appetite).	
2. Evaluate and approve proposed IT risk tolerance thresholds against the program's acceptable risk and opportunity levels.	
3. Determine the extent of alignment of the IT risk strategy to program risk strategy.	
4. Proactively evaluate IT risk factors in advance of pending strategic program decisions and ensure that risk-aware program decisions are made.	
5. Determine that IT use is subject to appropriate risk assessment and evaluation, as described in relevant international and national standards.	
6. Evaluate risk management activities to ensure alignment with the program's capacity for IT-related loss and leadership's tolerance of it.	

Governance Practice:	**Best Practice ID:**
Direct risk management - Direct the establishment of risk management practices to provide reasonable assurance that IT risk management practices are appropriate to ensure that the actual IT risk does not exceed the board's risk appetite.	EDM03-BP2
Review Activities:	
1. Promote an IT risk-aware culture and empower the program to proactively identify IT risk, opportunity and potential business impacts.	
2. Direct the integration of the IT risk strategy and operations with the program strategic risk decisions and operations.	
3. Direct the development of risk communication plans (covering all levels of the program) as well as risk action plans.	
4. Direct implementation of the appropriate mechanisms to respond quickly to changing risk and report immediately to appropriate levels of management, supported by agreed-on principles of escalation (what to report, when, where and how).	
5. Direct that risk, opportunities, issues and concerns may be identified and reported by anyone at any time.	

Governance Practice:	**Best Practice ID**
Monitor risk management - Monitor the key goals and metrics of the risk management processes and establish how deviations or problems will be identified, tracked and reported for remediation.	EDM03-BP3
Review Activities:	
1. Monitor the extent to which the risk profile is managed within the risk appetite thresholds.	
2. Monitor key goals and metrics of risk governance and management processes against targets, analyze the cause of any deviations, and initiate remedial actions to address the underlying causes.	
3. Enable key stakeholders' review of the program's progress towards identified goals.	
4. Report any risk management issues to the board or executive committee.	

Governance Practice:	Best Practice ID
Maintain a standard approach for program and project management - Maintain a standard approach for program and project management that enables governance and management review and decision making and delivery management activities focused on achieving value and goals (requirements, risk, costs, schedule, quality) for the business in a consistent manner.	BAI01-BP1
Manage stakeholder engagement - Manage stakeholder engagement to ensure an active exchange of accurate, consistent and timely information that reaches all relevant stakeholders. This includes planning, identifying and engaging stakeholders and managing their expectations.	BAI01-BP3
Launch and execute the program - Launch and execute the program to acquire and direct the resources needed to accomplish the goals and benefits of the program as defined in the program plan. In accordance with stage-gate or review criteria, prepare for stage-gate, iteration or release reviews to report on the progress of the program and to be able to make the case for funding up to the following stage-gate or release review.	BAI01-BP5
Monitor, control and report on the program outcomes - Monitor and control program (solution delivery) and enterprise (value/outcome) performance against plan throughout the full economic life cycle of the investment. Report this performance to the program steering committee and the sponsors.	BAI01-BP6
Manage program and project quality - Prepare and execute a quality management plan, processes and practices, aligned with the QMS that describes the program and project quality approach and how it will be implemented. The plan should be formally reviewed and agreed on by all parties concerned and then incorporated into the integrated program and project plans.	BAI01-BP9
Manage program and project risk - Eliminate or minimize specific risk associated with programs and projects through a systematic process of planning, identifying, analyzing, responding to, and monitoring and controlling the areas or events that have the potential to cause unwanted change. Risk faced by program and project management should be established and centrally recorded.	BAI01-BP10
Monitor and control projects - Measure project performance against key project performance criteria such as schedule, quality, cost and risk. Identify any deviations from the expected. Assess the impact of deviations on the project and overall program, and report results to key stakeholders.	BAI01-BP11

Introduction to Value Delivery

The IV&V team analyzed the following areas of value delivery for the Federally-Facilitated Marketplace (FFM) software product: code violations found through static code analysis using Sonar; system and acceptance testing; defect trends and management process, and closure of defects. Static code analysis is the analysis of computer source code that is performed without actually executing programs (analysis performed on executing programs is known as dynamic analysis or testing). The findings from code violations are not necessarily correlated with the defects identified during testing since testing is primarily focused on whether or not functionality is present and working correctly; whereas static code analysis is performed on the internal structure of the code and its maintainability. Problems with internal structure of code may not be found until an end user does something unexpected to cause an untested branch of code to be executed. In the case of FMPS, where only some of the test cases have been executed, it is likely that many structural problems will be found by end users and those who must maintain the code.

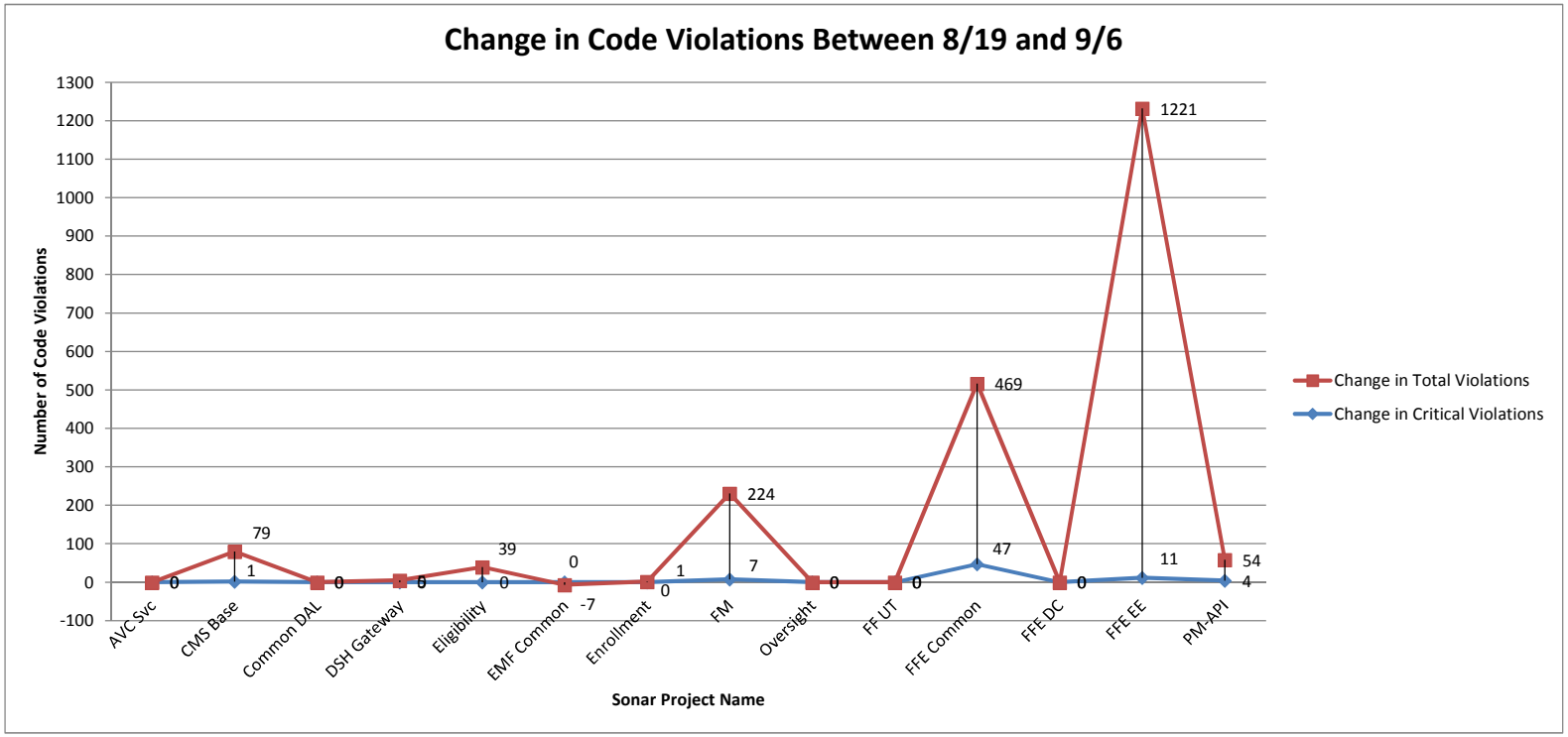
Gaps:

DEV001 -The *CheckStyle* and *Findbugs* plugins, and *Blocker* violations are not used in Sonar Quality Profile.
DEV002 -As per the CGI IQ Defect tracker dated 09/09/13 (doc50758) there were 1884 defects for which the root cause is "*Coding Not Per Requirement/Design*." The reason may be in the following areas: problems with requirements, lack of clarity of design or a developer training issue.
DEV003 -The sheer number of defects indicates poor code quality. For example, there were a total of 45 critical and 324 serious defects across all modules . There are 14 critical and 40 serious defects open this week .There were 597 *Section 508* defects, and 22 cross-browser defects per the CGI IQ Defect tracker (doc5118).
DEV004 - Many critical and major violations exist in the FFM code (i.e. empty catch blocks, improper class loader, etc.) which impacts the maintainability of the code. In addition, none of the projects has reviewed these critical violations yet.
DEV005 - Hardcoded values are spread out instead of being in a central place.
DEV006 - There are numerous naming convention violations.
DEV007 - The code contains one hardcoded IP address.
DEV008 - In the AVC SOAP WS Service (tags/PRIME_090613_01), code duplications are high. This is a maintainability issue.
DEV009 - An analysis of code violations between 8/19/13 and 9/6/13 showed that the same levels of code violations exist.
DMT001 - Some business capability areas have higher numbers of defects than others. These are: My Account, Individual Application, and Plan Compare.
TST001 - There were changes migrated to production without ACA testing in lower environments.
TST002 - Some of the changes only get ½ hr. for testing before getting migrated to upper environment.
TST003 - There are no Testing or Coding controls being enforced, which allow development contractors access to migrate code to production.
TST004 - Unable to locate the UAT test plans and results documentation within CALT.

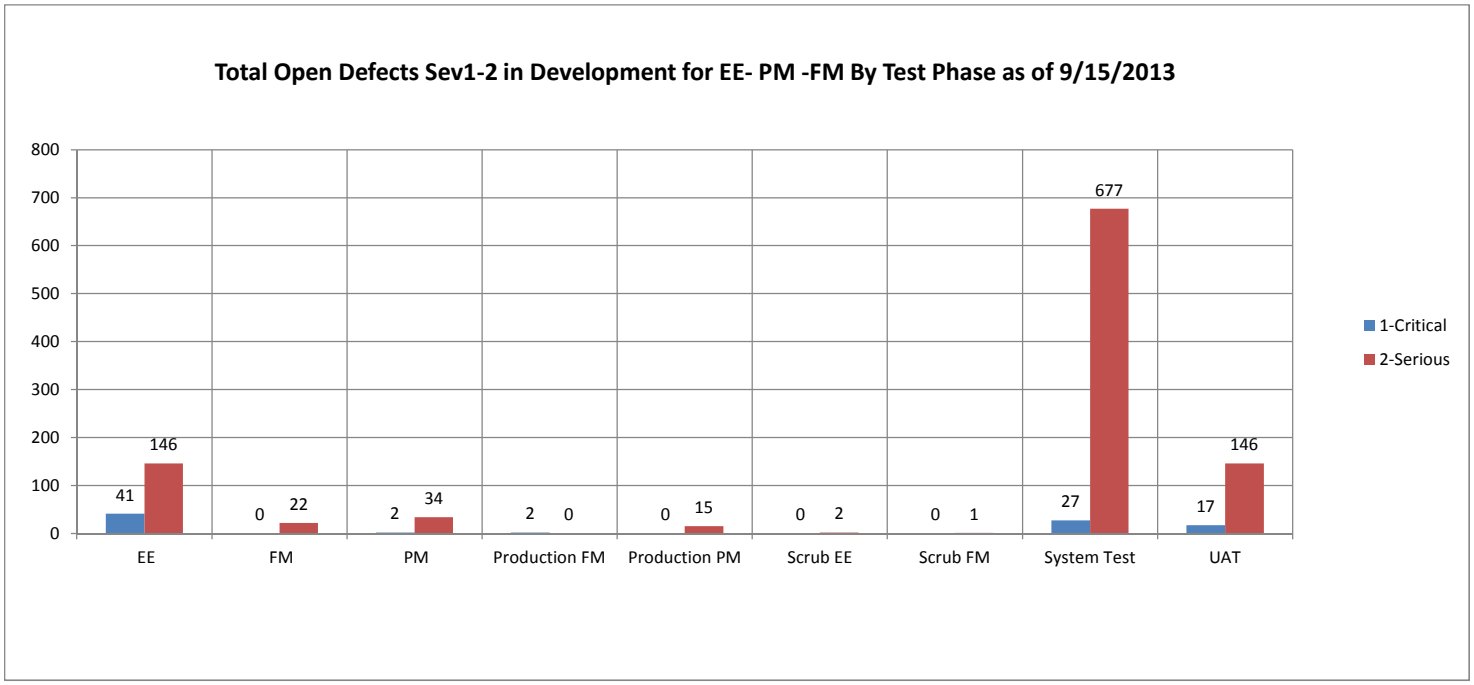
Recommendations:

DEV001 -Use the Sonar tool to perform reviews of the code. It is easier and more efficient to remove code violations before the code is delivered for testing.
DEV002 -Include *CheckStyle*, *Findbugs* and *Blocker* violation checks in Sonar Quality Profile.
DEV003 -All the confusions about requirements or design should be cleared through meetings prior to coding, and the defects should be fixed as soon as possible.
DEV004 -Review and fix the defects. Review and fix the violations.
DEV005 -Follow test driven-development and improve the coverage of code with unit tests.
DEV006 -Create a class or package of constants, so that the code is easier to maintain.
DEV007 -Follow the Java naming conventions and fix the naming convention issues with the code.
DEV008 -Replace the hardcoded IP address with a constant variable.
DEV009 -Remove the duplications in code by creating common functions and utility classes.
DEV010 - Review the critical defects still open at Go-Live and staff the Call Center accordingly.
DMT001 -Ensure resources are allocated to the appropriate areas of risk or modules with higher defects.
TST001 - Completion of testing must be verified as part of release management when software is moved to the Production environment**.**
TST002 - Adequate time to complete testing with complete test coverage needs to be scheduled and followed before migrating the program to the next environment.
TST003 - Controls for release management need to be published and followed.

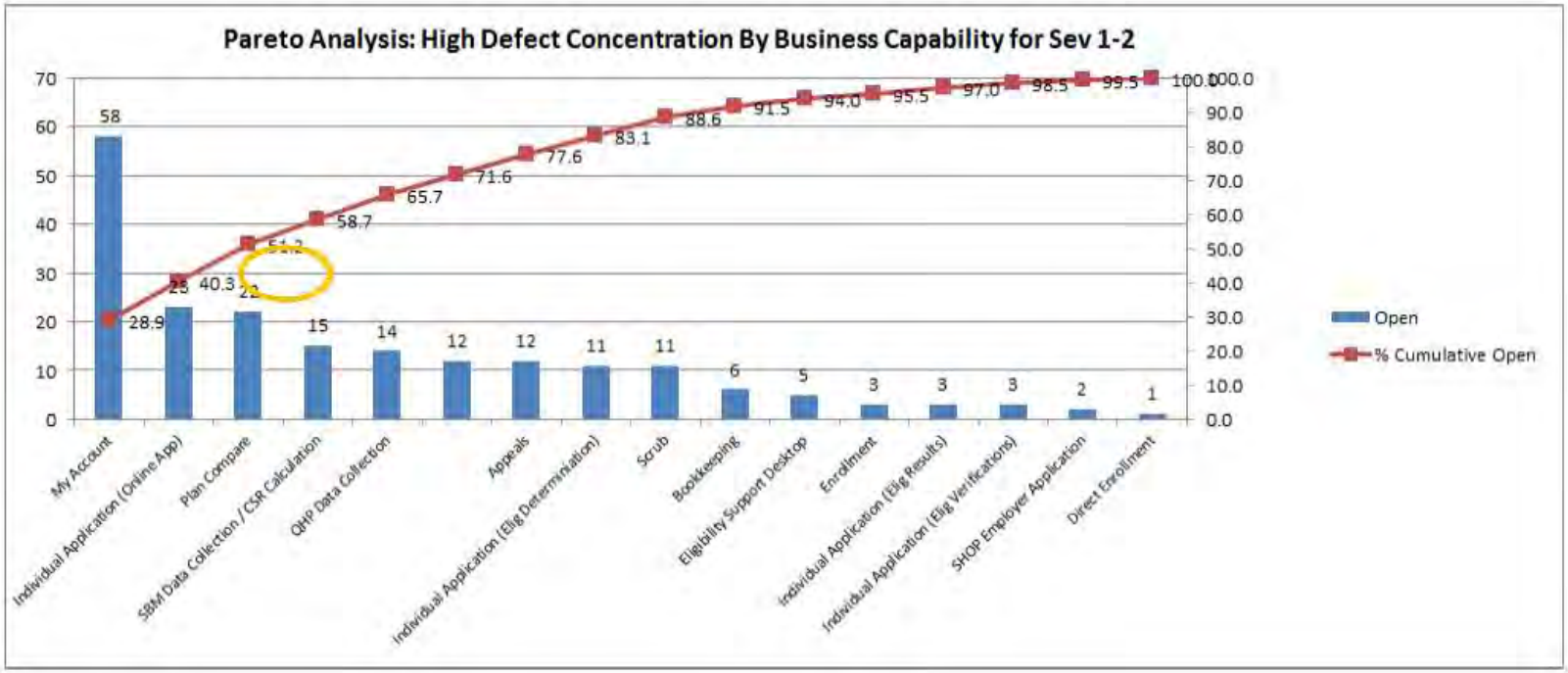
The FMPS program has established the Sonar tool as the static code analysis tool for the program. It is a simple process to use the tool to review the source code, and it should be a part of the developer's code peer reviews. This quality check can ensure a greater quality of code than testing, because test cases are not exhaustive. However, testing is still needed to ensure functionality meets requirements. The following graph depicts the change in code violations between 8/19/13 and 9/6/13 while defects identified through testing are being fixed. For the most part there has been a corresponding increase in the total code violations along with the lines of code. However, critical code violations have been roughly the same during this same period of time. Only in the EMF Common code, was there a decrease in the number of critical code violations. The FFM development team appears to be producing roughly the same quality code in terms of code violations. Please refer to Appendixes on code violations for additional



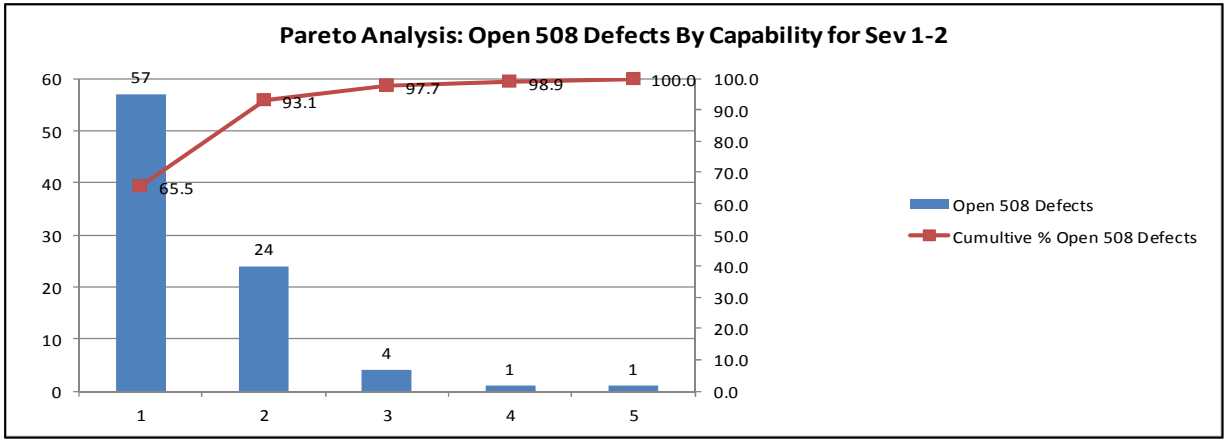
This following graph shows the total number of open severity 1 and 2 defects still in development as of 9/15/2013 for EE, FM, and PM by Test Phase. It is expected that the highest number of defects should be in system test, but 677 serious defects less than 2 weeks before the October Go-Live is high number. The 146 serious defects found in UAT should be closed as soon as possible. Note: Defects in the "Scrub" category are in the process of being updated by CGI. If 1% of the end users are impacted by open critical defects, then call volume could be



Pareto analysis is used to determine the location of the largest number of issues. Sometimes called, the 80/20 rule, the theory is that 80% of the problems are located in 20% of the modules. The following chart is based on the 9/15/2013 CGI Defect Extract of the open critical and serious defects for EE, FM and PM, by business capability. The bars are listed in decreasing order of number of defects in preparation for Pareto analysis. This chart shows that 51.2 % of the critical and serious defects are concentrated in 18% of the business capabilities (where there are 16 total business capabilities listed on the Y axis). The same three components are shown as the location of the greatest number of defects.



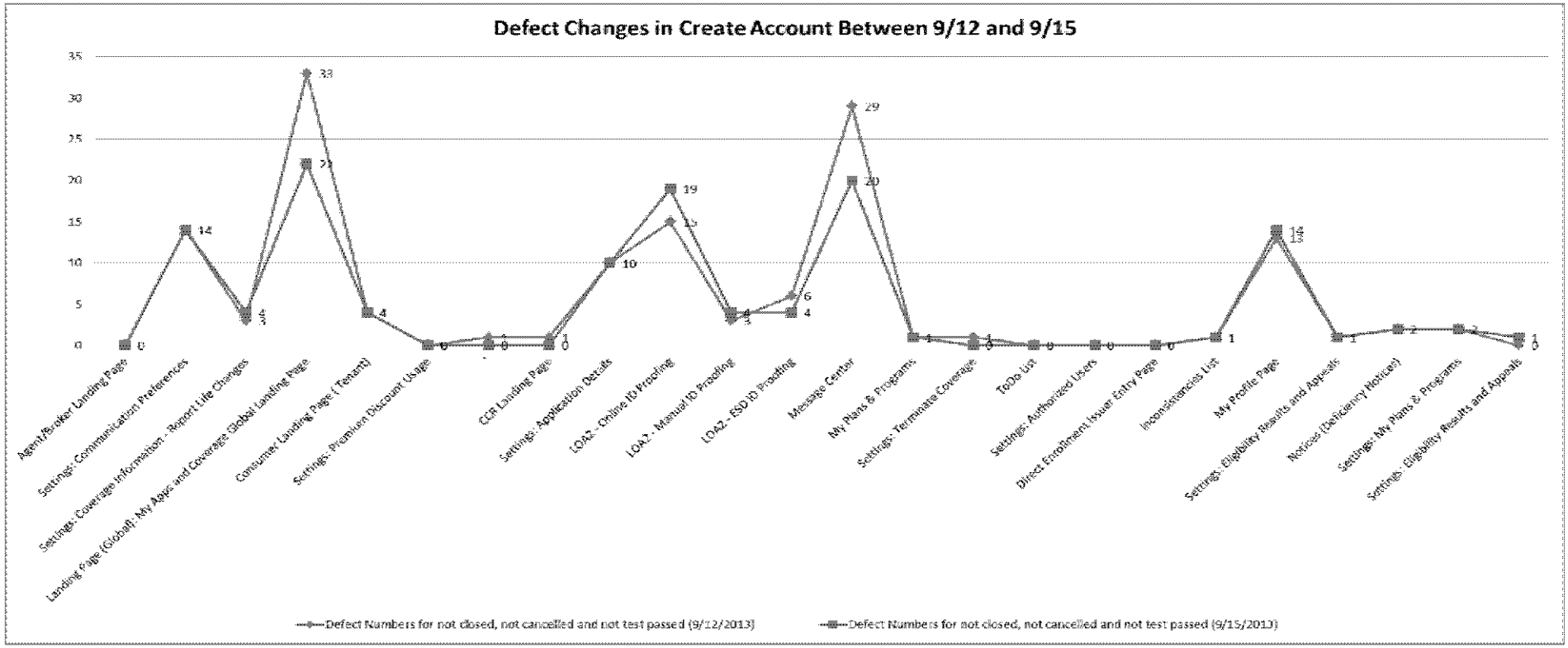
Pareto analysis is used to determine the location of the largest number of issues. Sometimes called, the 80/20 rule, the theory is that 80% of the problems are located in 20% of the modules. The following chart is based on the open and new, severity 1 and 2 Section 508 defects . Since Accessibility of Electronic and Information Technology (EIT) Section 508 is the law, these defects should be closed before the designated code freeze date.



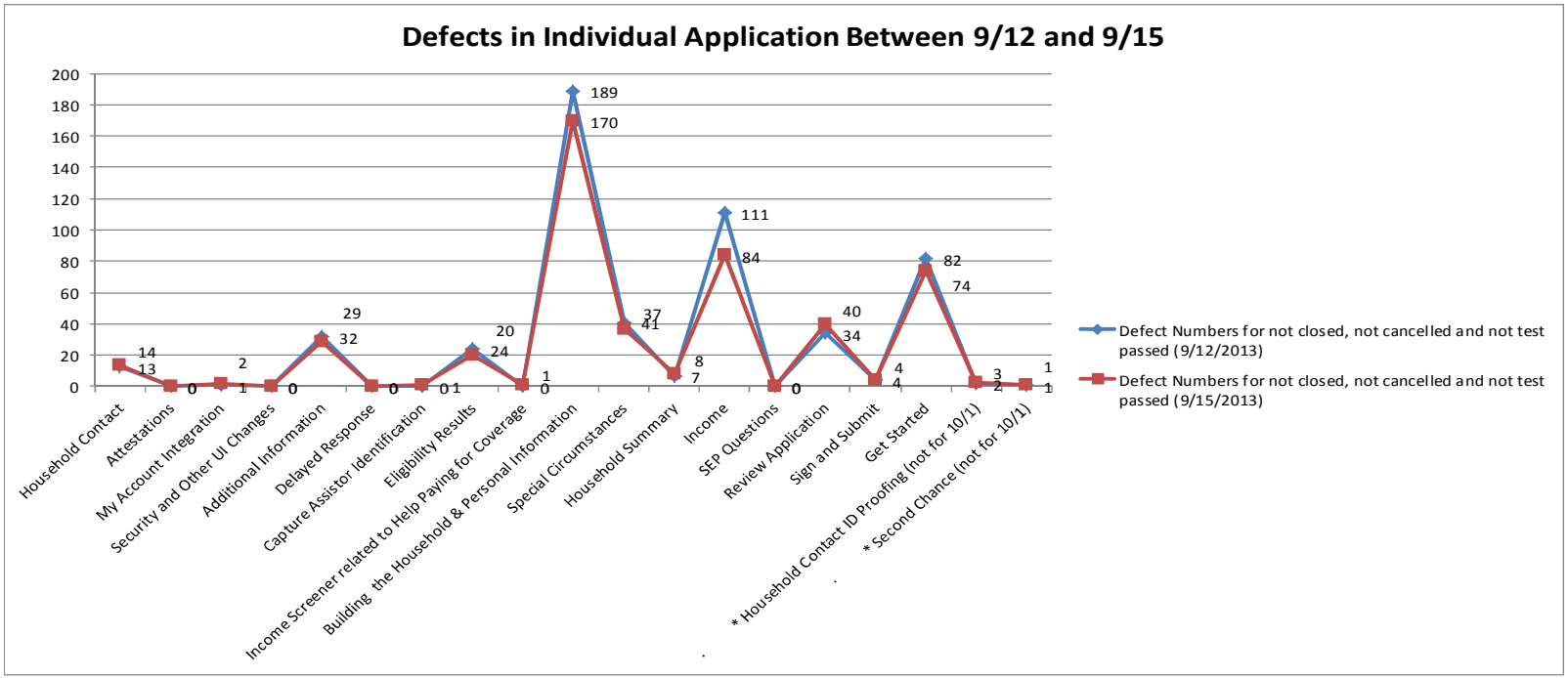
The following chart shows the root cause of all of the defects (open and closed as of 9/9/13) as documented by the development team. More than 47% of the defects have as a root cause, "Coding is not per requirement/design." This may be a problem with the requirements, the training of the developers or the approach/process by which the developers work. The column labeled "blank" represents no identified root cause analysis.

Count of ID	Colum																				
Row Labels		Coding Not Per Requirement /Design	Coding Standard Violation	Data Definition Error	Database/ Schema Design Error	Environment Issue	Error Handling Problem	Incorrect Application of Class, Macro or Function	Logical Design Error	Missing Requirements	Misstated Requirements	Requirements Baseline/Changes	Scrub	Syntax error	System Interface Design Error	Test Data Issues	Undetermined	User error	User Interface Design Error	(blank)	Grand Total
⊞	48																				48
⊞ EE	374	1292	69	4	3	22	1	2	3	21	5	11	52	1	2	4	539	1	4	225	2635
⊞ FM	35	296	11	6		2	6		3	8		1	14	2		1	85		7	74	551
⊞ Mainframe																				3	3
⊞ PM	37	296	25	1	10	4	4	1	12	6	1	1	37	1			161	3		85	685
⊟ Scrub			1										1				58			8	68
Plan Compare													1								1
(blank)			1														58			8	67
Grand Total	494	1884	106	11	13	28	11	3	18	35	6	13	104	4	2	5	843	4	11	395	3990

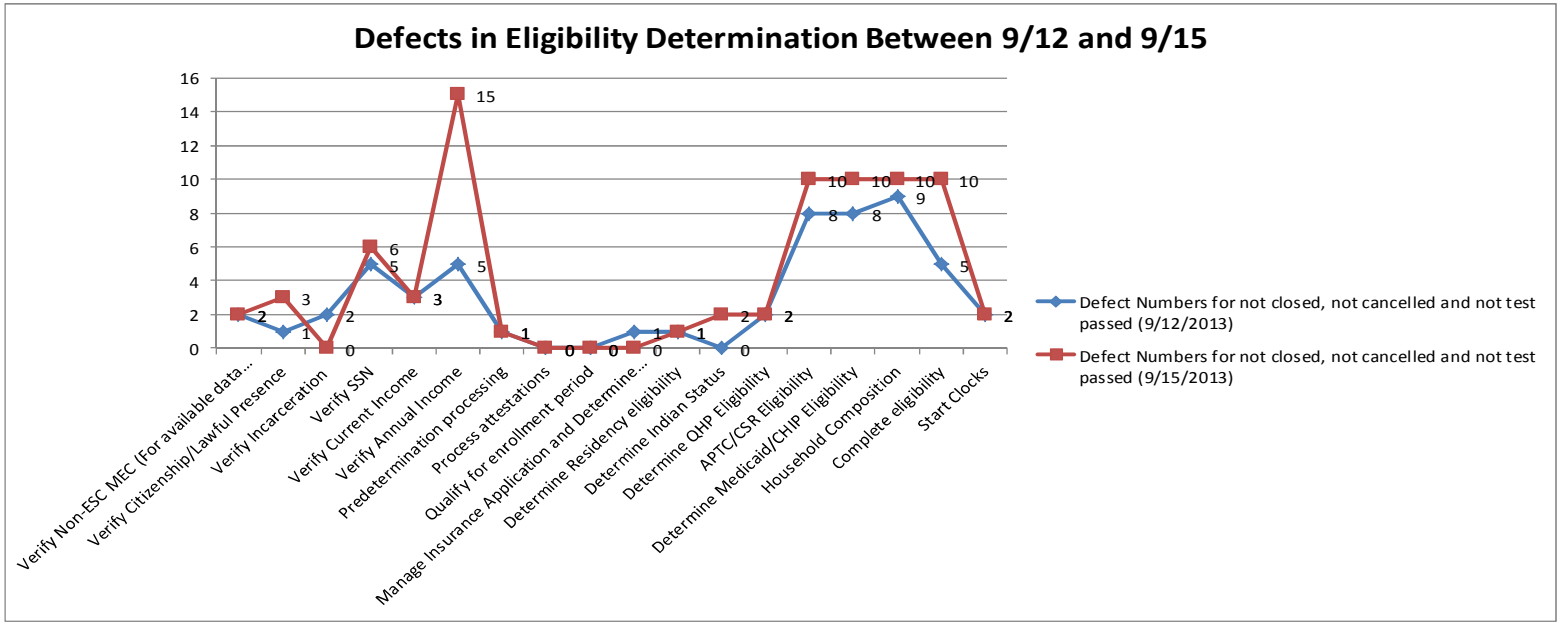
The following chart is a plot of defect changes in the Create Account business capability between 9/12 and 9/15. In most cases, defect numbers have remained the same. For Message Center and Landing Page, the defects have decreased. LOA2, Online ID Proofing defects have increased.



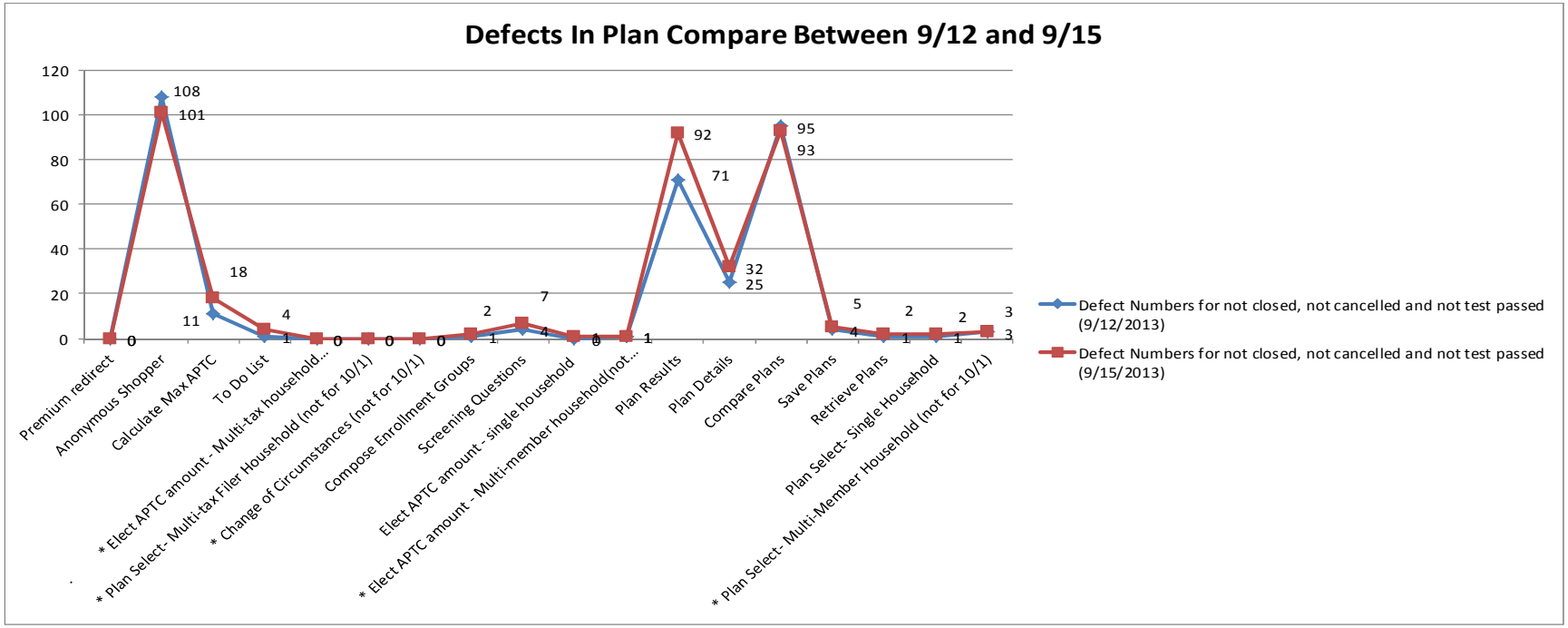
The following chart is a plot of defect changes in the Individual Application business capability between 9/12 and 9/15. Defect number are for all open types, including, not closed, not canceled, and testing not passed. In most cases, defect numbers have remained the same. For Income Screener and Income, the defects have decreased.



The following chart is a plot of defect changes in the Eligibility Determination capability between 9/12 and 9/15. Defect number are for all open types, including, not closed, not canceled, and testing not passed. In most cases, defects have increased. When defects are shown to increase over a period of time of testing, it is an indication of a design problem.



The following chart is a plot of defect changes in the Plan Compare capability between 9/12 and 9/15. Defect number are for all open types, including, not closed, not canceled, and testing not passed. In most cases, defects have remained the same. For Plan Results, the defects have decreased.



Risk Rating by Evaluation Category:	Average of Risk Probability (P)	Average of Risk Impact (I)	Average of Risk Score (P x I)	Average Risk Level	Risk Description Summary	Additional Risk Details	Recommendation
1. Is there an appropriate level of test coverage achieved by the test process?	4	4	16	HIGH	There were changes migrated to production without ACA testing in lower environments.	There were changes migrated to production without ACA testing in lower environments. There were two documented instances for FM 8/30 changes taken into prod on 9/2/2013 as well as FM bug fixes taken to prod on 9/11/2013.	Completion of testing must be verified as part of release management when software is moved to the Production environment.
2. Verify that an appropriate level of test coverage is achieved by the test process and that the correct code configuration has been tested.	3	4	12	MODERATE	Some of the changes only get ½ hr for testing before getting migrated to upper environment	Paul Donohoe mentioned on 9/12/2013 Testing Status meeting that he was told by Deepak that some of the changes only get ½ hr for testing before getting migrated to upper environment. Changes are not getting tested long enough before getting migrated, which results in increased rework and redeployment of objects.	Adequate time to complete testing with complete test coverage needs to be scheduled and followed before migrating the program to the next environment
3 Evaluate the procedures used for integration testing of system modules.	4	4	16	HIGH	There are no Testing or Coding controls being enforced, which allow development contractors access to migrate code to production.	There are no Testing or Coding controls being enforced, which allow development contractors access to migrate code to production. Only certain IDs should be able to migrate code to upper environments. There's no separation of duties.	Controls for release management need to be published and followed.
4 Evaluate interface testing plans and procedures for compliance with industry standards	3	3	9	MODERATE	Unable to locate the UAT test plans and results documentation within CALT	Could not review because unable to locate the UAT test plans and results documentation within CALT.	Documentaion needs to be made available to ensure that test coverage for UAT testing is complete and accurate
5 Verify that appropriate acceptance testing based on the defined acceptance criteria is performed satisfactorily before acceptance of software products.	4	4	16	HIGH	Unable to tie what's included in internal release testing to ACA release testing.	As of 9/15/2013, Unable to tie what's included in internal release testing to ACA release testing. On the CGI side: They provide RTM, release plans at the User Story level, Test Cases, Test Summary and Defect reports… But can't seem to locate the same granular level for ACA test for any releases after 7/31 and therefore, it's hard to link plans and results of these compliment testing.	Provide the summary and defect reports that tie testing to the user stories so that test coverage can be reviewed.

High	Moderate	Low

Value Delivery Control Objectives: APO11; BAI01; BAI06; BAI10; EDM02; BAI03 (COBIT)

1. Reduce solution and service delivery defects and rework - APO11
2. Meet quality standards with respect to Development Processes, Release Management Processes, Defect Management Processes and Test (planning, execution) activities. APO11
3. Define and communicate quality requirements in all processes, procedures and the related enterprise outcomes, including controls, ongoing monitoring, and the use Of proven practices and standards in continuous improvement and efficiency efforts. - APO11
4. Ensure the consistent delivery of solutions and services to meet the quality requirements of the enterprise and satisfy stakeholder needs. - APO11
5. Realize business benefits and reduce the risk of unexpected delays, costs and value erosion by improving communication to and involvement of business and end users, ensuring the value and quality of project deliverables, and maximizing their contribution to the investment and services portfolio. - BAI01
6. Manage all changes in a controlled manner, including standard changes and emergency maintenance relating to business processes, applications and infrastructure. This includes change standards and procedures, impact assessment, prioritization and authorization, emergency changes, tracking, reporting, closure and documentation. - BAI06
7. Enable fast and reliable delivery of change to the business and mitigation of the risks of negatively impacting the stability or integrity of the changed environment. - BAI06
8. Define and maintain descriptions and relationships between key resources and capabilities required to deliver IT-enabled services, including collecting configuration information, establishing baselines, verifying and auditing configuration information, and updating the configuration repository. - BAI10
9. Provide sufficient information about service assets to enable the service to be effectively managed, assess the impact of changes and deal with service incidents. - BAI10
10. Optimize the value contribution to the business from the business processes, IT services and IT assets resulting from investments made by IT at acceptable costs. - EDM02
11. Establish and maintain identified solutions in line with enterprise requirements covering design, development, procurement/sourcing and partnering with suppliers/vendors. Manage configuration, test preparation, testing, requirements management and maintenance of business processes, applications, information/data, infrastructure and services.- BAI03
12. Establish timely and cost-effective solutions capable of supporting enterprise strategic and operational objectives.- BAI03

Program Outcomes: APO11.01 - APO11.03; BAI01-O2; BAI01-O3; BAI01-O4; BAI01-O6; BAI10-O1; EDM02-O1 - EDM02-O2; BAI03-O3 (COBIT)

1. Development satisfies established quality standards with respect to code coverage, code quality, unit testing, project schedule (Path) promotion dates, etc...
2. Release Management satisfies quality and completeness criteria with respect to obtaining signature approval at established checkpoints prior to code promotion to test, UAT and Prod environments, build & release notes completeness, project schedule (Path) promotion dates, etc...
3. Test Management satisfies established quality standards with respect to test planning, test execution, test coverage, test status reporting, project schedule (Path) completion dates, etc...
4. Defect Management satisfies established quality standards with respect to defect management, defect recording, defect reporting and defect communication.
5. The scope and outcomes of the program are viable and aligned with program objectives.
6. The program and project activities are executed according to the plans.
7. Program and project plans are likely to achieve the expected outcomes.
8. Configuration repository is accurate, complete and up to date.
9. The program is securing optimal value from its initiatives, services and assets.
10. Optimal value is derived from IT investment through effective value management practices in the enterprise.
11. The program is realizing optimal value from the management processes or practices.
12. The solution conforms to the design, is in accordance with organizational standards, and has appropriate control, security and auditability.
13. The solution is of acceptable quality and has been successfully tested.

Inputs:

1. Generally Accepted Best Practices
2. Approved quality reviews - BAI02-WP9
3. Quality assurance plan - BAI03-WP7
4. Quality review results, exceptions and corrections - BAI03-WP8
5. QMS roles, responsibilities and decision rights - APO11-WP1
6. Quality management plans - APO11-WP2
7. Results of QMS effectiveness reviews - APO11-WP3
8. Quality management standards - APO11-WP4
9. Acceptance criteria - APO11-WP6
10. Results of quality reviews and audits - APO11-WP8
11. Results of solution and service delivery quality monitoring - APO11-WP10
12. Root causes of quality delivery failures - APO11-WP11
13. Approved acceptance test plan - BAI07-WP4
14. Risk analysis results - AP012-WP6
15. Risk mitigation actions - BAI02-WP7
16. Approved acceptance and release for production - BAI07-WP8
17. Identified quick wins - BAI05-WP8
18. Actions to improve value delivery - EDM02-WP6
19. Requirements for stage-gate reviews - EDM02-WP4
20. Identified supplier (contractor) delivery risk - APO10-WP7
21. Project performance criteria - BAI01-WP24
22. Project plans - BAI01-WP14
23. Project baseline - BAI01-WP15
24. Stage-gate review results - BAI01-WP13
25. Actions to improve value delivery - EDM02-WP6
26. Test plan - BAI03-WP9
27. Test procedures - BAI03-WP10

COBIT Process Name:	COBIT Process ID:	Associated Gaps
Manage Quality	APO11	DEV001
Manage Programs and Projects	BAI01	
Manage Changes	BAI06	
Manage Configuration	BAI10	
Ensure Benefits Delivery	EDM02	
Manage Solutions Identification and Build	BAI03	

COBIT Governance Practice:	COBIT Best Practice ID:
Monitor value optimization - Monitor the key goals and metrics to determine the extent to which the program is generating the expected value and benefits. Identify significant issues and consider corrective actions.	EDM02-BP3
Evaluate value optimization - Continually evaluate the portfolio of IT-enabled services and assets to determine the likelihood of achieving program objectives and delivering value at a reasonable cost. Identify and make judgment on any changes in direction that need to be given to management to optimize value creation.	EDM02-BP1
Establish a quality management system (QMS) - Establish and maintain a QMS that provides a standard, formal and continuous approach to quality management for information, enabling technology and business processes that are aligned with business requirements and program quality management.	APO11-BP2
Focus quality management on customers - Focus quality management on customers by determining their requirements and ensuring alignment with the quality management practices.	APO11-BP3
Perform quality monitoring, control and reviews - Monitor the quality of processes and services on an ongoing basis as defined by the QMS. Define, plan and implement measurements to monitor customer satisfaction with quality as well as the value the QMS provides. The information gathered should be used by the process owner to improve quality.	APO11-BP4
Integrate quality management into solutions for development and service delivery - Incorporate relevant quality management practices into the definition, monitoring, reporting and ongoing management of solutions development and service offerings.	APO11-BP5
Maintain continuous improvement. Maintain and regularly communicate an overall quality plan that promotes continuous improvement. This should include the need for, and benefits of, continuous improvement - Collect and analyze data about the QMS, and improve its effectiveness. Correct non-conformities to prevent recurrence. Promote a culture of quality and continual improvement.	APO11-BP3
Design high-level solutions - Develop and document high-level designs using agreed-on and appropriate phased or rapid agile development techniques. Ensure alignment with the IT strategy and program architecture. Reassess and update the designs when significant issues occur during detailed design or building phases or as the solution evolves. Ensure that stakeholders actively participate in the design and approve each version.	BAI03-BP1
Design detailed solution components. Develop, document and elaborate detailed designs progressively using agreed-on and appropriate phased or rapid agile development techniques, addressing all components (business processes and related automated and manual controls, supporting IT applications, infrastructure services and technology products, and partners/suppliers). Ensure that the detailed design includes internal and external SLAs and OLAs.	BAI03-BP2
Develop solution components - Develop solution components progressively in accordance with detailed designs following development methods and documentation standards, quality assurance (QA) requirements, and approval standards. Ensure that all control requirements in the business processes, supporting IT applications and infrastructure services, services and technology products, and partners/suppliers are addressed.	BAI03-BP3

Perform quality assurance (QA) - Develop, resource and execute a QA plan aligned with the QMS to obtain the quality specified in the requirements definition and the program's quality policies and procedures.	BAI03-BP6
Prepare for solution testing - Establish a test plan and required environments to test the individual and integrated solution components, including the business processes and supporting services, applications and infrastructure.	BAI03-BP7
Execute solution testing - Execute testing continually during development, including control testing, in accordance with the defined test plan and development practices in the appropriate environment. Engage business process owners and end users in the test team. Identify, log and priorities errors and issues identified during testing.	BAI03-BP8
Manage changes to requirements -Track the status of individual requirements (including all rejected requirements) throughout the product life cycle and manage the approval of changes to requirements.	BAI03-BP9

Senate Committee Staff Analysis of TurningPoint IVV Assessment 12. Lines in blue were added by Senate staff.

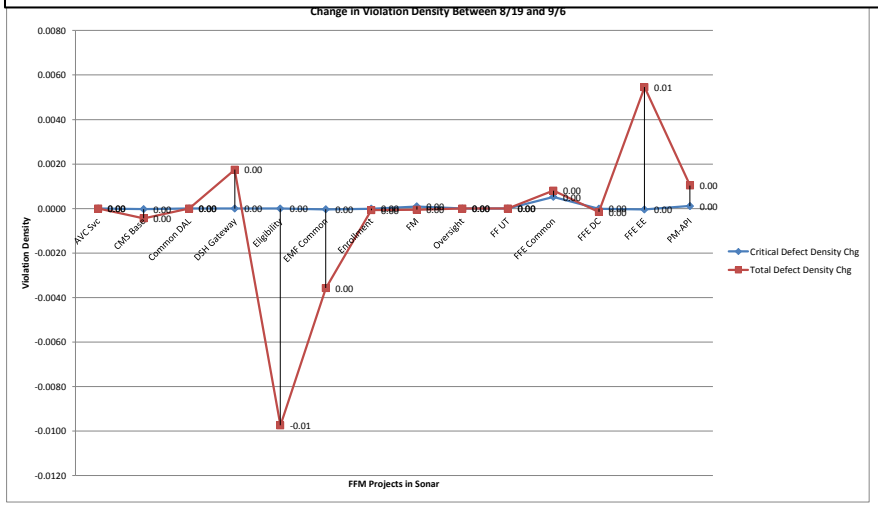
[redacted]

Introduction

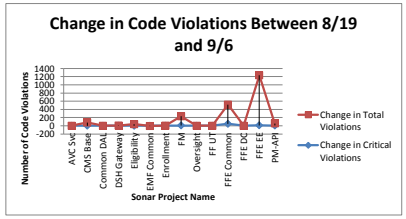
For this report, the IV&V team reviewed all of the code checked into SVN on 8/19/13 and 9/6/13. The graph below shows that there is a proportional number of violations i n the new lines of code from IV&V Assessment #11. The yellow indicates areas of change from the previous assessment. There is no evidence that code violations are being given attention.

Project	Short Name	Lines of Code	Crit Defect Density		Total Defect Density		Lines of Code	Crit Defect Density		Total Defect Density				Classes	Classes	Number of Critical Violations	Number of Critical Violations	SD-14, Total Number of Violations	SD-14, Total Number of Violations	SD-13, Comments %	SD-13, Comments %	Dulications %	Dulications %	Complexity (Number/Method)
Date		8/19/2013	8/19/2013	Lines with critical defects	8/19/2013	Lines with defects	9/6/2013	9/6/2013	Critical defects	9/6/2013	Lines with defects	Critical Defect Density Chg	Total Defect Density Chg	8/19/2013	9/6/2013	8/19/2013	9/6/2013	8/19/2013	9/6/2013	8/19/2013	9/6/2013	8/19/2013	9/6/2013	8/19/2013
AVC SOAP WS Service (tags/PRIME7_081913_01/PRIME_090613_01 version 6.2)	AVC Svc	1030	0.39%	4	1.55%	16	1030	0.39%	4	1.55%	16	0.00%	0.00%	6	6	4	4	16	16	8.2	8.2	55.5	55.5	10.5
CMS Base Project (tags/PRIME7_081913_01/PRIME_090613_01 version 7.0)	CMS Base	64406	0.17%	108	6.00%	3862	66211	0.16%	109	5.95%	3941	0.00%	-0.04%	871	895	108	109	3862	3941	12.7	12.7	7.5	7.7	3.3
Common DAL (tags/PRIME7_081913_01/PRIME_090613_01 version 1.2)	Common DAL	904	0.22%	2	9.40%	85	904	0.22%	2	9.40%	85	0.00%	0.00%	18	18	2	2	85	85	12.8	12.8	0	0	3.4
DSH Gateway Project (tags/PRIME7_082113_02/PRIME_090613_01 version 7.0)	DSH Gateway	1990	0.00%	0	7.49%	149	2010	0.00%	0	7.66%	154	0.00%	0.17%	36	36	0	0	149	154	26	26.2	4.4	5.2	4.2
Eligibility (tags/PRIME7_081913_01/PRIME_090613_01 version 7.0)	Eligibility	773	0.00%	0	5.30%	41	1848	0.00%	0	4.33%	80	0.00%	-0.98%	10	16	0	0	41	80	16.5	11.7	13	16.2	2.8
EMF Common (tags/PRIME7_081913_01/PRIME_090613_01 version 7.0)	EMF Common	2690	0.30%	8	8.07%	217	2724	0.29%	8	7.71%	210	0.00%	-0.36%	47	49	8	8	217	210	16.8	16.7	1	1	2.7
Enrollment (tags/PRIME7_081913_01/PRIME_090613_01 version 7.0)	Enrollment	1335	0.07%	1	9.14%	122	1347	0.07%	1	9.13%	123	0.00%	-0.01%	11	11	1	1	122	123	10.2	10.1	8.2	8.1	4.4
FF FM Project (tags/PRIME7_081913_01/PRIME_090613_01 version 7.0)	FM	41698	0.10%	41	7.96%	3321	44542	0.11%	48	7.96%	3545	0.01%	-0.01%	599	635	41	48	3321	3545	15.9	16.2	8.9	9	3.6
FF Oversight URR Project (tags/PRIME7_081913_01/PRIME_090613_01)	Oversight	23888	0.08%	19	5.80%	1386	23888	0.08%	19	5.80%	1386	0.00%	0.00%	267	267	19	19	1386	1386	8.2	8.2	10.2	10.2	5.3
FF UT Project (tags/PRIME7_081913_01/PRIME_090613_01 Version 6.2)	FF UT	2200	0.05%	1	4.95%	109	2200	0.05%	1	4.95%	109	0.00%	0.00%	24	24	1	1	109	109	6.1	7.3	6.1	6.1	5.4
FFE Common Project (tags/PRIME7_080313_01/PRIME_090213_03 Version 7.0)	FFE Common	55393	0.20%	110	5.78%	3199	62644	0.25%	157	5.86%	3668	0.05%	0.08%	464	526	110	157	3199	3668	23.1	22.4	9.4	8.8	7.1
FFE DC Project (tags/PRIME7_082113_02/PRIME_090613_01 Version 6.2)	FFE DC	31163	0.28%	86	6.61%	2061	31237	0.28%	86	6.60%	2061	0.00%	-0.02%	290	291	86	86	2061	2061	10.4	10.3	9.3	9.4	6.2
FFE EE Project (tags/PRIME7_082113_02/PRIME_090913_01 version 7.0)	FFE EE	69573	0.07%	50	3.48%	2419	90496	0.07%	61	4.02%	3640	0.00%	0.55%	534	665	50	61	2419	3640	16.3	16.9	8.3	9.8	5.8
PM-API (tags/PRIME7_082113_02/PRIME_090613_01 version 7.0)	PM-API	23123	0.32%	74	6.67%	1542	23567	0.33%	78	6.77%	1596	0.01%	0.10%	281	284	74	78	1542	1596	11.4	11.2	15.2	15.3	3.8
		320,166	0.16%	504	5.79%	18,529	354,648	0.16%	574	5.81%	20,614	4.432E-05	0.0002521											

The following graph depicts the change in code violation density between 8/19/13 and 9/6/13 (as defects from testing are bein g corrected). A negative number indicates decreased code violation density and a positive number indicates increased code violation density. Overall, there has been little change in defect den sity. For the Eligibility Sonar project, there was decreased *Total Code Violation Density* of -.01. However, there were only 1,848 lines of code present in the Eligibility Sonar project on 9/6/13. This translates to app roximately 18 fewer code violations than were present at 8/19. In actuality, there were a total of 41 Total Code Violations on 8/18/13 for 773 lines of code and now there are 80 Total Code Violations for 1,848 lines of code. On the other hand, for the FFE EE Sonar Project, which showed an increase in Total Density of .00545 with 90,496 lines of code, representing an increase of 1221 violations.



Short Name	Change in Critical Violations	Change in Total Violations
AVC Svc	0	0
CMS Base	1	79
Common DAL	0	0
DSH Gateway	0	5
Eligibility	0	39
EMF Common	0	-7
Enrollment	0	1
FM	7	224
Oversight	0	0
FF UT	0	0
FFE Common	47	469
FFE DC	0	0
FFE EE	11	1221
PM-API	4	54



[redacted]

Exhibit 8

QSSI. Federal Exchange Program System Data Service Hub Statement of Work. Sept. 30, 2011. SFC-0000000280.

3. Participating in a collaborative environment and relationship to support the coordination between CMS and the primary partners, e.g., the Internal Revenue Service (IRS)

The foregoing activities must be completed to ensure the DSH will be ready. The following reviews represent the key milestones (stage gate reviews in the ELC, dates represented as calendar year) for the DSH:

- Architecture Review: October 2011
- Project Startup Review: Q4 2011
- Project Baseline Review: Q4 2011
- Preliminary Design Review: Q1 2012
- Detailed Design Review: Q1 2012
- Final Detailed Design Review: Q2 2012
- Pre-Operational Readiness Review: Q2 2012
- Operational Readiness Review: Q3 2012

A detailed description of the foregoing activities and milestones can be found in the *Collaborative Environment and Life Cycle Governance Supplement to the Exchange Reference Architecture: Foundation Guidance* document and the CMS ILC site at http://www.cms.hhs.gov/SystemLifecycleFramework/

The planned artifacts and templates for the FEPS development will also be stored in the Application Life Cycle Management (ALM) environment that CMS is standing up for the use of multiple stakeholders across the Affordability Care Act projects.

1.3 Assumptions and Constraints

The Contractor shall take the following assumptions and constraints into consideration:

- The Affordable Care Act requires individuals to be enrolled in appropriate health insurance programs by January 2014. CMS expects open enrollment to begin in October 2013. CMS requires that Exchange and DSH capability be ready for nationwide testing by January 2013.
- The DSH will need to be developed and available to support state information exchange testing with various federal entities. In addition, CMS requires full functionality of the DSH to be designed, developed, and implemented by September 1st, 2013.
- The DSH will be utilized by other HHS agencies for shared services. For example, Community Living Assistance Services and Supports (CLASS) will utilize the DSH to conduct Eligibility verifications with other federal agencies.
- Varying schedules among participants within overall Exchange Program. Other federal agency partners and the states will determine their own development and delivery schedules for their components of the program.

Highly Confidential and Proprietary Business Records
Produced Pursuant to Senate Rule XXVI

QSSI-SFC-0000000280

81

Exhibit 9

Emails among CMS Officials. QSSI-ECC-0000036602–QSSI-ECC-0000036603. Sept. 27, 2013.

Message

From: Chao, Henry (CMS/OIS) [redacted]

Sent: 9/26/2013 10:51:10 AM

To: Booth, Jon G. (CMS/OC) [redacted]; Linares, George E. (CMS/OIS) [redacted]; Akhtar Zaman [redacted] Couts, Todd (CMS/OIS) [redacted]; Outerbridge, Monique (CMS/OIS) [redacted] Patel, Ketan (CMS/OC) [redacted]; Fasching, Laura [redacted]; Rich Schwarzkopf [redacted] Um, Peter (CMS/CTR) [redacted] Thurston, Robert (CMS/CTR) [redacted]; Margush, Doug C. (CMS/OIS) [redacted]; Skinner, Dennis R. (CMS/OIS) [redacted]; Yousef Shahegh (CMS/OIS) [redacted] Royle, Erick B. (CMS/OIS) [redacted]; Venkat Basavaraju [redacted]; Carter, Cathy T. (CMS/OIS) [redacted]; Marc Richardson [redacted] Outerbridge, Monique (CMS/OIS) [redacted]; Grothe, Kirk A. (CMS/OIS) [redacted]; O'Kussick, James J. (CMS/OIS) [redacted]; Murray, Ruairi S. (CMS/OIS) [redacted]; Oh, Mark U. (CMS/OIS) [redacted]

CC: Winthrop, Monica (CGI Federal) [redacted]; Sharma, Hemant (CGI Federal) [redacted]; Karlton Kim [redacted] Michael Finkel [redacted]; Campbell, Cheryl (CGI Federal) [redacted]; Keith Rubin [redacted]; Van, Hung B. (CMS/OIS) [redacted]; Stephen Walter [redacted] George Schindler [redacted]; Stevenson, Corey B. (CMS/OIS) [redacted]; Gray, Edward M. (CMS/OIS) [redacted] Donna Ryan [redacted] Snyder, Michelle (CMS/OA) [redacted] Trenkle, Tony (CMS/OIS) [redacted]; Igor Rafalovich [redacted]; Jason Hase [redacted]

Subject: FW: FFM UI PST results & Concrens on System Peformances

Attachments: Summary of PST activities for Monday; PST Summary for Tuesday; PST Summary for Wednesday; Update: PST Summary for Wednesday

Importance: High

Just talked to Jon and it looks like the bar for hc.gov on the learn side is set at 10k concurrent users. I would say that post October 1st the peaks will be at 50k or greater and the Get Insured side for consumers will be at least the same and likely more, and then to compound the demand on the internal FFM architecture to support the call center (web services to the online application) plus the fetching person view by Serco all need to be factored in to a meaningful assessment and test of performance and ability to sustain HA without having a meltdown starting at only 10k on the get insured side.

The coordination for demand on the FFM architecture and Hub also needs to have the network (internal to the cloud, external to the cloud to the Internet, and external to the cloud to CMSNet plus the replication to HP) and all other factored computed to some mathematical expression of total and partial part of the architecture theoretical

capacity. Add other overhead such as security, monitoring, OS level and Application level services such as EFT to the total as well to get a full picture.

George and Akhtar will be working with Jon and Ketan and with all the architects and TMRK/Verizon/URS to get me and answer today (the calculated total and partial capacities of the architecture) and then move quickly to coordinate a set of test to stress the systems to find the breakpoints now.

Monica and CGI Team—I need to know which environment will be the place where we will do this performance testing at the peaks I mentioned—that means the infrastructure folks and the architects have to have the configurations set correctly and triple checked for every element that affects availability and performance.

Separately I need Monique to get this in sync with any necessary execution of temporary and longer term agreements to supply and be able to spawn greater capacity on demand and get that ironed out now—I DO NOT WANT A REPEAT OF WHAT HAPPENED NEAR THE END OF DECEMBER 2005 WHERE MEDICARE.GOV HAD A MELTDOWN (THIS IS TO GET YOUR ATTENTION IF I DIDN'T HAVE IT ALREADY. IF you even detect the slightest need for more compute at TMRK or at HP or both then work on a plan to get it temporarily or permanent if needed.

I expect to see something planned and ready to execute by 6-7pm this evening.

Henry Chao
Deputy CIO & Deputy Director,
Office of Information Services
Centers for Medicare & Medicaid Services
[redacted]

From: Chao, Henry (CMS/OIS)
Sent: Thursday, September 26, 2013 9:09 AM
To: 'Campbell, Cheryl (CGI Federal)'; Rich Martin [redacted] George Schindler [redacted]
Cc: Outerbridge, Monique (CMS/OIS); Oh, Mark U. (CMS/OIS); Van, Hung B. (CMS/OIS)
Subject: FW: FFM UI PST results & Concrens on System Peformances
Importance: High

George
Cheryl
Rich,

I am going to raise this at the 9am so be ready with a response on how we will together focus on getting performance up to at least 10k or greater concurrent users without defects, which will stop us from ever finishing performance testing.

THanks

Henry Chao
Deputy CIO & Deputy Director,
Office of Information Services

Centers for Medicare & Medicaid Services
[redacted]

From: Zaman, Akhtar (CMS/OIS)
Sent: Thursday, September 26, 2013 8:50 AM
To: Oh, Mark U. (CMS/OIS); Margush, Doug C. (CMS/OIS); Thurston, Robert (CMS/CTR); Basavaraju, Venkat (CMS/OIS); Walter, Stephen J. (CMS/OIS); Shao, Lijun (CMS/CPI); Van, Hung B. (CMS/OIS)
Cc: Donohoe, Paul X. (CMS/OIS); Grothe, Kirk A. (CMS/OIS); Outerbridge, Monique (CMS/OIS); Chao, Henry (CMS/OIS)
Subject: FFM UI PST results & Concrens on System Peformances

Hi All,

We ran several Performance & Stress Test (PST) cycles (starting from 10 Vuser to 2000 Vuser) since last 3 days but the results are not good and not consistent at all (see attached PST results between 09/23-09/25). The only success we had on **Monday (09/23)** when we ran a 500 VUser cycle and received acceptable response time (<5 sec) for all the FFE individual application transactions except **Race & Ethnicity** which took about **65 sec.** Pls note that our focus was limited to Individual application submission, and since we didn't get the appropriate eligible results (stuck with "Almost finished" issue), we couldn't continue to Plan results & enrollments. During this test only **1**[redacted] was used in AZ.

CGI identified the high RT for the Race & Ethnicity and applied a hotfix – which I believe mainly fine tune the [redacted] associated with the Race and Ethnicity step. Then we repeated the same **500** Vusers test on **Tuesday (09/24),** and received good results – the **Race & Ethnicity** took only **4sec.** Also Tuesday's test was involved **10**[redacted] in AZ. Then we attempted a **2000** Vuser cycle but all the users failed immediately while accessing the Homepage with "Service Temporary Unavailable" error and the test was stopped. CGI determined that some of the requests were not going to the right [redacted] nodes. A [redacted] issue was routing traffic to a [redacted] server which was down.

On **Wednesday (09/25)** we started with the **500** VUser cycle using **10**[redacted] configuration – which was an attempt to replicate the results of the successful **500** Vuser test that was run on Tuesday. But the test finished with a lot of errors. The Individual App, Race and Ethnicity Transactions were taking a long time and eventually the system reached a breakpoint, after which everything started failing. CGI said they were investigating a problem in how the messages are being sent across the cluster under load.

> CGI decided that they would like to run a test routing everything to 1[redacted] Server to verify that all transactions are working. We ran a 250 Vuser cycle and received mixed results (**187 success** & 123 failed transactions, mainly login failures). CGI reported that they reviewed the logs from the test and had changed property files and needed to bounce the servers. We ran a 500 VUser cycle, didn't observe any Login failures but system reached a breakpoint within 6 minutes after which the response time started increasing rapidly and users started failing with HTTP Status-Code=502 (Proxy Error). CGI reported that they had identified an issue in MarkLogic and applied another Hotfix by the end of the day.
>
> Later in the Wednesday evening, we ran two more cycles of testing. We attempted two cycles at **2,000** Vusers. Neither was successful. The results were as follows:
>
> > Cycle 1
> > 2000 Vuser test (8:40 pm)
> > Large number of Race and Ethnicity failures.

CGI suspects a load balancing issue. Made changes and restored the database.

Cycle 2
2000 Vusers (9:31 pm)
Saw very high Login response times. As the vusers ramped up there were a large number of login failures. Test was stopped.

We'll have a technical group meeting today (09/26, 3-4pm) to review the recent Performance & Stress Testing (PST) results along with the performance metrics collected and shared by TRMRK & others. We need to summarize what has been achieved so far and what not and the strategy to continue PST in one of our Implementation environment. Also what's our takeaway from the recent PST findings towards the production configuration for 10/01.

Finally the only positive news is the PST between Hub & TDS (SSA, IRS & EES) went pretty good, and we hit the target SLA (**93 TPS with SSA, 40 TPS with IRS & 32 TPS with EES**) and the average response time was below **2 seconds** (about 1.7 sec).

Pls feel free to share any related questions/concerns on the above summary,

Akhtar

This electronic mail (including any attachments) may contain information that is privileged, confidential, and/or otherwise protected from disclosure to anyone other than its intended recipient(s). Any dissemination or use of this electronic email or its contents (including any attachments) by persons other than the intended recipient(s) is strictly prohibited. If you have received this message in error, please notify the sender by reply email and delete the original message (including any attachments) in its entirety.

Message

From: Zaman, Akhtar (CMS/OIS) [redacted]
Sent: 9/27/2013 2:35:50 PM
To: Jim Jones [redacted] Deepak Bhatta [redacted] Natarajan, Venkatesan (CMS/CTR) [redacted]
Subject: FW: Terremark RedSeal Topology Map

From: Sharma, Hemant (CGI Federal) [redacted]
Sent: Friday, September 27, 2013 2:23 PM
To: Chao, Henry (CMS/OIS)
Cc: Outerbridge, Monique (CMS/OIS); Zaman, Akhtar (CMS/OIS); Um, Peter (CMS/CTR); Oh, Mark U. (CMS/OIS)
Subject: RE: Terremark RedSeal Topology Map

Hi Henry,

Here are my observations/reactions to the email from Dave and building on top of Akhtar's email:

1. The scripts are failing so far due to issues like load balancing, inefficient and defective code, and inefficient queries.
    a. Let me enumerate the primary issues we have run into so far in our performance tests:
        i. Incorrect setup of the application zone load balancer which caused only one of the two [redacted] servers to be recognized. This was fixed for subsequent performance test runs.
        ii. Inefficient [redacted] for person matching. The [redacted] was tuned and baselined.
        iii. The generation of identifiers within MarkLogic was inefficient. This was fixed and verified as part of the 500 user test.
    b. At this time we have not identified any inefficient and defective code as part of the performance test.
    c. We tried to run a 2000 user test but ran into issues with the generation of identifies in Marklogic again. We have since fixed this but it needs to be tested in the next performance test.
2. Adding capacity to address bottlenecks like these will likely be ineffective.
    a. The defects enumerated above are very typical in any performance test and part of the tuning exercise. However, we were able to capture metrics from the tests that indicate the following:
        i. There is the opportunity to add more capacity to the [redacted] servers to support higher volume of users.
        ii. Each of the [redacted] servers will have a certain capacity to support concurrent requests – based on our tests the floor seems to be 250 users per application zone [redacted]. We don't have a value for the ceiling, but our best guess would be 500 or so concurrent users. Based on this, the current configuration would likely support 10K concurrent users and we would benefit from an increase in the number of [redacted] servers.
3. While a patch has been developed to fix what we believe is the current bottleneck (the Application ID) we currently have no way to test it and will likely run into the next bottleneck far short of what the equipment and VM's are capable of supporting.
    a. As Akhtar mentioned, we will be testing in the [redacted] environment.
    b. We should be able to verify the fix for the generation of identifiers.
    c. We may find other issues during our performance testing – we will find and fix these issues as we encounter them. This is a typical performance test cycle.
4. There are also plans to scale [redacted] by adding VMs, but currently the environment has only a single VM.

a. [redacted] currently has two [redacted], three application [redacted], one [redacted], four data [redacted], and 3 large [redacted] for Marklogic.
b. Further, we will be increasing the capacity for [redacted] to continue with our performance test efforts.

5. This will make it even more difficult to extrapolate and forecast performance once it is operational.
   a. I believe that performance test results can be extrapolated based on results from the [redacted] environment for the production environment.
   b. We will continue to increase the number of users in performance testing as well as the functionality that is tested.

Please let me know if there are any questions of concerns.

Thanks,
Hemant

Hemant Sharma | Vice President, CGI Federal | [redacted] www.cgi.com
CONFIDENTIALITY NOTICE: Proprietary/Confidential Information belonging to CGI Group Inc. and its affiliates may be contained in this message. If you are not a recipient indicated or intended in this message (or responsible for delivery of this message to such person), or you think for any reason this message may have been addressed to you in error, you may not use or copy or deliver this message to anyone else. In such case, you should destroy this message, and are asked to notify the sender by reply email.

From: Zaman, Akhtar (CMS/OIS) [redacted]
Sent: Friday, September 27, 2013 1:36 PM
To: Chao, Henry (CMS/OIS); Um, Peter (CMS/CTR); Oh, Mark U. (CMS/OIS); Sharma, Hemant (CGI Federal)
Cc: Outerbridge, Monique (CMS/OIS)
Subject: RE: Terremark RedSeal Topology Map

I can add my feedback, and Hemant & Peter can correct me and add more

We're planning to move to [redacted] from today to continue our performance testing, troubleshooting, tuning etc. Also I believe CGI will move the fixes for the performance bottlenecks in [redacted] today and we can verify it as a part of our PST tonight. We'll continue our PST in [redacted] for next few weeks

Based on my knowledge, [redacted] already have 3 [redacted] in each zone (AZ, DZ, & ML) from FFM side and 8 VMs on DSH/HUB side – which we believe is good starting point to continue testing/troubleshooting. And our goal is to bump up the capacity to at least half of the production (say 8-10VMs per zone) asap to continue the 10k concurrent user load testing and ultimately we're expecting [redacted] to be full production sizes to reach our ultimate goal of 50k concurrent user testing. Also we're planning for a single VM testing (1/1/1) to establish some benchmark for the concurrent user capacity that we can use as a baseline for estimating the possible no of VMs needed to support 50k concurrent user load testing.

We're working on the PST data strategy using both TH & TDS options to continue our PST. We'll need your support to extend the SSA & IRS testing window (connecting to their Test/Integration env) till we have the PST data loaded into the TH. I believe SSA is fine connecting to their Integration env as of now but not IRS where we need your help. Pls feel free to let me know any related question/concerns. Thx,

Akhtar

From: Chao, Henry (CMS/OIS)
Sent: Friday, September 27, 2013 1:10 PM
To: Um, Peter (CMS/CTR); Oh, Mark U. (CMS/OIS); Zaman, Akhtar (CMS/OIS); 'Hemant.Sharma[redacted]
Cc: Outerbridge, Monique (CMS/OIS)
Subject: Fw: Terremark RedSeal Topology Map
Importance: High

Can one of you please correct Dave's assessment and write the reasons why and get back to me in the next hour?

Henry Chao
Deputy Chief Information Officer and Deputy Director
Office of Information Services
Centers for Medicare & Medicaid Services
[redacted]

From: Nelson, David J. (CMS/OEM)
Sent: Friday, September 27, 2013 01:02 PM
To: Chao, Henry (CMS/OIS)
Subject: RE: Terremark RedSeal Topology Map

Henry,

From my perspective. This is not a theoretical capacity planning exercise. I am confident your team of architects have thoughtfully worked through capacity sizing (VMs, CPUs, Memory, Storage, Network, etc.) based on assumptions such as efficient code.

The performance test results in [redacted] are based on the 10[redacted]. The scripts are failing so far due to issues like load balancing, inefficient and defective code, and inefficient queries. We have not been successful in moving beyond 500 concurrent users filling applications without income verification. Adding capacity to address bottlenecks like these will likely be ineffective. We must give ourselves the ability to work through these tuning issues and at this point we do not have an operational environment for further performance testing.

While a patch has been developed to fix what we believe is the current bottleneck (the Application ID) we currently have no way to test it and will likely run into the next bottleneck far short of what the equipment and VM's are capable of supporting.

We moved performance testing out of Prod Prime before it became Production and this environment is now connected to the Federal Partner production systems. The plan is to move performance testing to [redacted] which is not yet operational. There are also plans to scale [redacted] by adding VMs, but currently the environment has only a single VM. This will make it even more difficult to extrapolate and forecast performance once it is operational. Shoring up [redacted] and connecting it to the hub and the federal partner test environment needs to be a priority.

I realize everything is a priority but... the facts are that we have not successfully handled more than 500 concurrent users filling out applications in an environment that is similarly in size to Day 1 production. We cannot proactively find or replicate actual production capacity problems without an appropriately sized operational performance testing environment. And, we have not even started looking for tuning issues in the plan select and enroll parts of the application.

From: Chao, Henry (CMS/OIS)
Sent: Friday, September 27, 2013 11:13 AM
To: Um, Peter (CMS/CTR); Outerbridge, Monique (CMS/OIS); Oh, Mark U. (CMS/OIS); Margush, Doug C. (CMS/OIS); Sharma, Hemant (CGI Federal) [redacted] Keith Rubin; Karlton Kim [redacted]; Mike Finkel [redacted]; Linares, George E. (CMS/OIS); Skinner, Dennis R. (CMS/OIS); Thurston, Robert (CMS/CTR); Zaman, Akhtar (CMS/OIS); Patel, Ketan (CMS/OC); Fasching, Laura [redacted]; Nelson, David J. (CMS/OEM); Couts, Todd (CMS/OIS)
Cc: Berkley, Katrina (CMS/OIS); Rhones, Rhonda D. (CMS/OIS)
Subject: FW: Terremark RedSeal Topology Map
Importance: High

I want to use this as a basis for tracing where we would have performance bottlenecks and Hemant can add his analysis along with Akhtar's extrapolation off performance in a smaller sized environment. By 3pm I want to see an analysis and report describing performance using whatever you guys/gals come up with as a basis for measurement for the network from Akamai in and back out on learn and get insured sides, backside Hub to other agencies performance metrics, max/min for each part including shared parts of the architecture, steady state and burstable levels, and then translated to a performance and capacity framework Michelle and Jim can understand.

Todd will make sure this gets translated and packaged for our use and for Michelle and Jims consumption.

Henry Chao
Deputy CIO & Deputy Director,
Office of Information Services
Centers for Medicare & Medicaid Services
[redacted]

From: Schankweiler, Thomas W. (CMS/OIS)
Sent: Friday, September 27, 2013 10:43 AM
To: Chao, Henry (CMS/OIS)
Cc: Um, Peter (CMS/CTR); Margush, Doug C. (CMS/OIS); Oh, Mark U. (CMS/OIS); Thurston, Robert (CMS/CTR); Outerbridge, Monique (CMS/OIS)
Subject: FW: Terremark RedSeal Topology Map

Henry,

Just wanted to provide you with an overdue update you on a task that has been outstanding from security for a while now. Attached is the latest version of the RedSeal network map for Terremark. Folks are working each week to further refine the accuracy of the map. In addition, there have been 6 items identified which Terremark is working to resolve or provide more information on. Each of these are flagging as weaknesses against best practice hardening standards. The CISO's office is advised as they are the ones running the RedSeal program.

Tom

From: Sokoly, Joseph A.(CMS/CTR)
Sent: Friday, September 27, 2013 10:36 AM
To: Schankweiler, Thomas W. (CMS/OIS)
Subject: Terremark RedSeal Topology Map

Tom,

Attached is the most recent Terremark topology map that RedSeal has. Let me know if you have any trouble opening it or have any questions.

Thanks,
Joseph Sokoly
[redacted]

This electronic mail (including any attachments) may contain information that is privileged, confidential, and/or otherwise protected from disclosure to anyone other than its intended recipient(s). Any dissemination or use of this electronic email or its contents (including any attachments) by persons other than the intended recipient(s) is strictly prohibited. If you have received this message in error, please notify the sender by reply email and delete the original message (including any attachments) in its entirety.

Message

From: Zaman, Akhtar (CMS/OIS) [redacted]
Sent: 9/30/2013 4:09:09 PM
To: Donohoe, Paul X. (CMS/OIS) [redacted] Deepak Bhatta [redacted] Natarajan, Venkatesan (CMS/CTR) [redacted] Jim Jones [redacted]
Subject: FW: FFM Performance Discussion points

fyi

From: Zaman, Akhtar (CMS/OIS)
Sent: Monday, September 30, 2013 4:03 PM
To: Chao, Henry (CMS/OIS); Outerbridge, Monique (CMS/OIS); Grothe, Kirk A. (CMS/OIS); Oh, Mark U. (CMS/OIS); Walter, Stephen J. (CMS/OIS); Shao, Lijun (CMS/CPI); Basavaraju, Venkat (CMS/OIS); Van, Hung B. (CMS/OIS)
Subject: FFM Performance Discussion points

Hi Henry,

I'm trying to responding your e-mail yesterday regarding the FFM application performances.

Currently we are seeing performance degradation starting around **1100 - 1200** concurrent users, and most of the pages (except few) are responding within **10** seconds at that load. Few transactions/pages are taking longer such as **Application Summary Save, Family & household Summary Save, Race & Ethnicity etc.** – which should be investigated by the development team, and should be brought to the attention of Monitoring & Helpdesk team. As of today, we're only focusing on Individual application performance testing and going all the way to application submission. The plan is to continue testing to ramp up load to 10k concurrent users. Plan compare has not yet been tested. Currently we cannot get to Plan Compare because the plan data not loaded in [redacted] yet. Once available we can provide a page by page metrics for the entire application, registration as well as plan compare. Also Call Center and ESW load scenarios has not been added to the current performance testing because those are not available in current [redacted] code.

In addition to the FFM individual application performance testing we're conducting FFM-EIDM integration testing for [redacted] accounts creation and step-up to [redacted]. EIDM applied a hot-fixes last night (2am) on the "[redacted]-identification by-pass" which helping us to continue the [redacted] accounts PST. I believe we should focus on the [redacted] accounts creation performance testing today considering in first few weeks we may see more accounts creation than individual applications. So far we are able to create 2000 [redacted] accounts and step-up to [redacted] using 200 concurrent user load, and the average response time was below 4 seconds although the login was about 22 seconds.

The test we are running since last few days give us the limitation of each [redacted] servers. We definitely seen some improvements with increased capacity (# of [redacted], CPU, Java memory etc.) but still observing issues/bottlenecks with [redacted] load balancers/[redacted] in every run which needs additional investigation. If we do the plain math (based on the current statistics), the system is able to handle up to **1200** concurrent users with **4 app** [redacted] – which may require about **30 App** [redacted] to handle **10,000** concurrent users. And as we're only testing half of the total functionalities (excluding Plan results/compare, enrollments, CCR, ESD etc.) we should even apply a **2.x factor** in the estimated calculations – which would make about **60+ App** [redacted] to handle **10,000** concurrent users. I believe from data zone & ML prospect the overall CPU utilization looks much better, and may not require as high number of [redacted] as app zone. Bottom-line we need to focus more on application tuning (code, query optimization etc.) rather just increasing the infrastructures, otherwise by the time we shoot for 50,000 concurrent users we may run out .....

From performance testing prospect we would need to continue performance testing/troubleshooting in [redacted] by bumping concurrent users and also adding more VMs as we progressing. At the same time we would need to get the

most recent code in [redacted] and continue scripting for all other missing functionalities (Plan results/compare, enrollments, CCR, ESD etc.). We also need to work with Mathematica to get clean PST data loaded into Test Harness so that we get successful eligibility results and continue to plan results/compare. Our goal is to hit 10,000 concurrent users at first, and then keep shooting for the 50,000 concurrency limits.

Also you have asked to get performance metrics from OC & Akamai, and I have received below stats from Ketan. We'll try to analyze those and factor into our performance testing scenarios.

Below recent statistics based on September 26th which one the busiest day on Healthcare.gov which can provide you some details.

Sept 26th Stats:
Total Page views for the day: 3,857,489
Visits: 628,475
Avg Pages/Visit: 6.14
Avg Page Load Time: 3 sec.
Bandwidth consumption for the day: 1 TB.
Busiest Time of day : 11:00 am to 12:00 pm & 6:00 pm to 7:00 pm EST
Highest Concurrent users at the time of the day: 13,651.
During Peak at 6:45 pm bandwidth traffic: 410.46 mb/sec
During Peak at 6:45 pm request traffic: 1,199.9 req/sec
During Peak at 6:45 pm : 104 page/sec

We have bumped our Akamai bandwidth capacity to 50TB/month. We have purchased security features like WAF & Site shield to protect both Learn & Marketplace from DDoS and any application layer attacks. If we have to increase the bandwidth we can always do that. Learn side has no dependency on marketplace from capacity due to Akamai caching. All users will be first coming to Learn and then go to Marketplace. Learn will control all the incoming traffic to Marketplace.

Pls feel free to let me know any related questions/concerns, Thx,

Akhtar

-----Original Message-----
From: Chao, Henry (CMS/OIS)
Sent: Sunday, September 29, 2013 11:12 AM
To: Zaman, Akhtar (CMS/OIS); Outerbridge, Monique (CMS/OIS); Van, Hung B. (CMS/OIS); Oh, Mark U. (CMS/OIS); Walter, Stephen J. (CMS/OIS); Shao, Lijun (CMS/CPI); Basavaraju, Venkat (CMS/OIS)
Subject: Re: Discussion points
Importance: High

Akhtar,

I expect you to also have these answers as we continue testing deeper and wider and to help explain in business terms whether if we are:

Determining no degradation of performance for a given segment of testing such as plan compare (expected versus actual tolerance for consumer wait times, for example).

Determining where the degradation begins and the rate at which it begins to falter in delivering a function--this should include Web Services with Call center and Serco.

Making recommendations on adjustments to the architecture at the VM level or some other aspect--doing this in conjunction with the architects.

Working with the architects on determining recommendations for a final configured Prod environment to maximize performance based on what we see in current testing environments.

Working with OC and Akamai determining performance metrics and benchmarks including any dependencies from learn to get insured to we services.

Providing the written analysis and final determinations and estimates for performance in total and by process/function, and where we need to be aware and pre-emptively invoke messaging and/or throttling of users coming in to the online application.

Can you do this starting today (you are doing much of it already) and making some adjustment in how you lead this effort so that by tomorrow midday we have some semblance of a final picture of performance.

Thanks.

Henry Chao
Deputy Chief Information Officer and Deputy Director Office of Information Services Centers for Medicare & Medicaid Services
[redacted]

----- Original Message -----
From: Zaman, Akhtar (CMS/OIS)
Sent: Sunday, September 29, 2013 08:54 AM
To: Chao, Henry (CMS/OIS); Thurston, Robert (CMS/CTR); Outerbridge, Monique (CMS/OIS); 'george.schindler [redacted] 'Cheryl.Campbell [redacted] 'Hemant.Sharma [redacted] 'rich.martin [redacted] Van, Hung B. (CMS/OIS)
Subject: RE: Discussion points

I believe Hemant & CGI needs to address those questions based on the Performance testing run last night.

We'll be continue to test today, tomorrow & beyond until we reach at least 10k concurrent users, and eventually 50k. So far, we only covered the Individual application in PST, and today we'll be focusing on scripting Plan results, Plan compare, and enrollments. Also we'll be performance testing FFM-EIDM integration today.

-----Original Message-----
From: Chao, Henry (CMS/OIS)
Sent: Sunday, September 29, 2013 8:43 AM
To: Thurston, Robert (CMS/CTR); Zaman, Akhtar (CMS/OIS); Outerbridge, Monique (CMS/OIS); 'george.schindler [redacted] 'Cheryl.Campbell [redacted]; 'Hemant.Sharma [redacted] 'rich.martin [redacted]; Van, Hung B. (CMS/OIS)
Subject: Fw: Discussion points

These are Todd's questions.

Henry Chao
Deputy Chief Information Officer and Deputy Director Office of Information Services Centers for Medicare & Medicaid Services

[redacted]

----- Original Message -----
From: Park, Todd [redacted]
Sent: Sunday, September 29, 2013 08:23 AM
To: Chao, Henry (CMS/OIS)
Cc: Snyder, Michelle (CMS/OA)
Subject: Discussion points

Hi Henry, channeling my inner Michelle, a few questions (all of which I think she or I have floated at some point), perhaps for discussion at the 9 am or later today:

-- Has the team run performance/diagnostic testing on the whole FFM, so that we know that the Marklogic bottleneck is in fact the critical, rate-limiting one, as opposed to another bottleneck in, say, Plan Compare or elsewhere, that could also constrain the number of concurrent users?

-- In other words, does the performance testing the team is doing make you confident that the FFM across the board can indeed take 16,000 concurrent users, rising to 60,000-70,000 with the new hardware? - So far we were able to run 2000 concurrent users in [redacted], Hemant needs to

-- Are we going to run performance testing today and tomorrow on the growing aggregate collection of hardware (not just one unit of it), so we validate the projections of 16,000/60,000-70,000 with the actual production machinery?

-- Are we testing to make sure that incoming traffic gets properly load balanced across the VMs/units? (This may be accomplished by the previous item)

-- What happens after the 16,000/60,000-70,000 threshold is reached? Is there gradual degradation of response time for users? Rapid degradation? Immediate crashing?

Massive kudos again for the incredible progress the team is making!

This electronic mail (including any attachments) may contain information that is privileged, confidential, and/or otherwise protected from disclosure to anyone other than its intended recipient(s). Any dissemination or use of this electronic email or its contents (including any attachments) by persons other than the intended recipient(s) is strictly prohibited. If you have received this message in error, please notify the sender by reply email and delete the original message (including any attachments) in its entirety.

Message

From: Deepak Bhatta [redacted]

Sent: 9/29/2013 7:36:04 PM

To: Akhtar Zaman [redacted] Thurston, Robert (CMS/CTR)

Subject: FW: Venky/Deepak/Jim - Pls review!!!: Discussion points

Importance: High

Hey Thurston,

Can you please help with some of the answers below, especially regarding Akamai.

Akhtar, can you please reach out to OC and get some information as well? Below is what I got so far. Please make corrections as needed.

----------HENRY'S REQUEST----------

Akhtar,

I expect you to also have these answers as we continue testing deeper and wider and to help explain in business terms whether if we are:

Determining no degradation of performance for a given segment of testing such as plan compare (expected versus actual tolerance for consumer wait times, for example).

Currently we are seeing performance degradation starting around 1400 users in the race/ethnicity page. Other pages are responding with SLA (< 10 seconds) at that load. The plan is to ramp up load to 10k concurrent users. Plan compare has not yet been tested. Currently we cannot get to Plan Compare. Once available we can provide a page by page metrics for the entire application, registration as well as plan compare.

Determining where the degradation begins and the rate at which it begins to falter in delivering a function--this should include Web Services with Call center and Serco.

Call Center and ESW load has not been added to the current performance test. ESD functionality is not currently working. For call center we can add the call center APIs to the current load.

Making recommendations on adjustments to the architecture at the VM level or some other aspect--doing this in conjunction with the architects.

The test we are running today should give us the limitation of each [redacted] servers. As the FFM adds more servers today we should be able to determine the capacity of each server.

Working with the architects on determining recommendations for a final configured Prod environment to maximize performance based on what we see in current testing environments.

We will be working with CGI to determine the FFM capability per server and come up with a recommendation. We will be working with the architects from both FFM and HUB to determine the final capacity requirement.

Working with OC and Akamai determining performance metrics and benchmarks including any dependencies from learn to get insured to we services.
Thurston/Akhtar can you help with this?

Providing the written analysis and final determinations and estimates for performance in total and by process/function, and where we need to be aware and pre-emptively invoke messaging and/or throttling of users coming in to the online application.
Our plan is to have 54k applications/hr completed. Please add here as well.

Can you do this starting today (you are doing much of it already) and making some adjustment in how you lead this effort so that by tomorrow midday we have some semblance of a final picture of performance.

Deepak Bhatta | QSSI | www.qssinc.com
ACA – FFM Testing
[redacted]

-----Original Message-----
From: Zaman, Akhtar (CMS/OIS) [redacted]
Sent: Sunday, September 29, 2013 12:03 PM
To: Natarajan, Venkatesan (CMS/CTR); Deepak Bhatta; Jim Jones
Subject: Venky/Deepak/Jim - Pls review!!!: Discussion points
Importance: High

Pls see below e-mail from Henry, and I need your help to draft the response by today, pls put high priority on this, feel free to call me for any questions,

-----Original Message-----
From: Chao, Henry (CMS/OIS)
Sent: Sunday, September 29, 2013 11:12 AM
To: Zaman, Akhtar (CMS/OIS); Outerbridge, Monique (CMS/OIS); Van, Hung B. (CMS/OIS); Oh, Mark U. (CMS/OIS); Walter, Stephen J. (CMS/OIS); Shao, Lijun (CMS/CPI); Basavaraju, Venkat (CMS/OIS)
Subject: Re: Discussion points
Importance: High

Akhtar,

I expect you to also have these answers as we continue testing deeper and wider and to help explain in business terms whether if we are:

Determining no degradation of performance for a given segment of testing such as plan compare (expected versus actual tolerance for consumer wait times, for example).

Determining where the degradation begins and the rate at which it begins to falter in delivering a function--this should include Web Services with Call center and Serco.

Making recommendations on adjustments to the architecture at the VM level or some other aspect--doing this in conjunction with the architects.

Working with the architects on determining recommendations for a final configured Prod environment to maximize performance based on what we see in current testing environments.

Working with OC and Akamai determining performance metrics and benchmarks including any dependencies from learn to get insured to we services.

Providing the written analysis and final determinations and estimates for performance in total and by process/function, and where we need to be aware and pre-emptively invoke messaging and/or throttling of users coming in to the online application.

Can you do this starting today (you are doing much of it already) and making some adjustment in how you lead this effort so that by tomorrow midday we have some semblance of a final picture of performance.

Thanks.

Henry Chao
Deputy Chief Information Officer and Deputy Director Office of Information Services Centers for Medicare & Medicaid Services
[redacted]

----- Original Message -----
From: Zaman, Akhtar (CMS/OIS)
Sent: Sunday, September 29, 2013 08:54 AM
To: Chao, Henry (CMS/OIS); Thurston, Robert (CMS/CTR); Outerbridge, Monique (CMS/OIS); 'george.schindler [redacted] 'Cheryl.Campbell [redacted] 'Hemant.Sharma [redacted] 'rich.martin [redacted] Van, Hung B. (CMS/OIS)
Subject: RE: Discussion points

I believe Hemant & CGI needs to address those questions based on the Performance testing run last night.

We'll be continue to test today, tomorrow & beyond until we reach at least 10k concurrent users, and eventually 50k. So far, we only covered the Individual application in PST, and today we'll be focusing on scripting Plan results, Plan compare, and enrollments. Also we'll be performance testing FFM-EIDM integration today.

-----Original Message-----
From: Chao, Henry (CMS/OIS)
Sent: Sunday, September 29, 2013 8:43 AM
To: Thurston, Robert (CMS/CTR); Zaman, Akhtar (CMS/OIS); Outerbridge, Monique (CMS/OIS); 'george.schindler [redacted] 'Cheryl.Campbell [redacted] 'Hemant.Sharma [redacted] 'rich.martin [redacted] Van, Hung B. (CMS/OIS)
Subject: Fw: Discussion points

These are Todd's questions.

Henry Chao
Deputy Chief Information Officer and Deputy Director Office of Information Services Centers for Medicare & Medicaid Services
[redacted]

[redacted]

----- Original Message -----
From: Park, Todd[redacted]
Sent: Sunday, September 29, 2013 08:23 AM
To: Chao, Henry (CMS/OIS)
Cc: Snyder, Michelle (CMS/OA)
Subject: Discussion points

Hi Henry, channeling my inner Michelle, a few questions (all of which I think she or I have floated at some point), perhaps for discussion at the 9 am or later today:

-- Has the team run performance/diagnostic testing on the whole FFM, so that we know that the Marklogic bottleneck is in fact the critical, rate-limiting one, as opposed to another bottleneck in, say, Plan Compare or elsewhere, that could also constrain the number of concurrent users?

-- In other words, does the performance testing the team is doing make you confident that the FFM across the board can indeed take 16,000 concurrent users, rising to 60,000-70,000 with the new hardware? - So far we were able to run 2000 concurrent users in [redacted], Hemant needs to

-- Are we going to run performance testing today and tomorrow on the growing aggregate collection of hardware (not just one unit of it), so we validate the projections of 16,000/60,000-70,000 with the actual production machinery?

-- Are we testing to make sure that incoming traffic gets properly load balanced across the VMs/units? (This may be accomplished by the previous item)

-- What happens after the 16,000/60,000-70,000 threshold is reached? Is there gradual degradation of response time for users? Rapid degradation? Immediate crashing?

Massive kudos again for the incredible progress the team is making!

This electronic mail (including any attachments) may contain information that is privileged, confidential, and/or otherwise protected from disclosure to anyone other than its intended recipient(s). Any dissemination or use of this electronic email or its contents (including any attachments) by persons other than the intended recipient(s) is strictly prohibited. If you have received this message in error, please notify the sender by reply email and delete the original message (including any attachments) in its entirety.

Exhibit 10

TurningPoint. Federal Marketplace Program System (FMPS) Independent Verification & Validation (IV&V) Assessment 10 Report. Nov. 18, 2013.

CENTERS FOR MEDICARE & MEDICAID SERVICES

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

Federal Marketplace Program System (FMPS)

Independent Verification & Validation (IV&V) Assessment 10 Report

Version 2.0

November 18, 2013

Prepared by:

TurningPoint
TurningPoint Global Solutions
Software Services Company™

Document Number: FMPSIVV-IAR-10
Contract Number: HHSM-500-2012-00008U

APPROVALS

Marketplace IT Program Approving Authority:

Signature	Printed Name	Date	Phone Number

Monique Outerbridge, CMS/OIS/CIISG, Director

Signature	Printed Name	Date	Phone Number

Kirk Grothe, CMS/OIS/CIISG, Deputy Director

Signature	Printed Name	Date	Phone Number

Rhonda Rhones, CMS/OIS/CIISG, Government Task Lead

REVISION HISTORY

Version	Date	Organization/Point of Contact	Description of Change
1.0	11/13/2013	TurningPoint	Initial submission
2.0	11/18/2013	TurningPoint	Removed FDSH RM Findings that applied to FFM and were duplicated in FDSH Updated finding numbers in Table 1 and figures 2 and 3 Updated Figure 1 Removed duplicated OE finding from FDSH

Table of Contents

EXECUTIVE SUMMARY 1

1 INTRODUCTION 5

1.1 BACKGROUND 5
1.2 SCOPE 5
1.3 FMPS OVERVIEW 5
1.4 IV&V APPROACH AND METHODS 5
1.5 ASSUMPTIONS 7
1.6 CONSTRAINTS 7
1.7 REFERENCES 7

2 FFM 8

2.1 FFM QUALITY MANAGEMENT FINDINGS 8
2.2 FFM TRAINING FINDINGS 11
2.3 FFM REQUIREMENTS MANAGEMENT FINDINGS 14
2.4 FFM OPERATING ENVIRONMENT FINDINGS 18
2.5 FFM SOFTWARE DEVELOPMENT FINDINGS 20
2.6 FFM SYSTEM AND ACCEPTANCE TESTING FINDINGS 29
2.7 FFM DATA MANAGEMENT FINDINGS 36
2.8 FFM OPERATIONS OVERSIGHT FINDINGS 46

3 FDSH 49

3.1 FDSH QUALITY MANAGEMENT FINDINGS 49
3.2 FDSH TRAINING FINDINGS 51
3.3 FDSH REQUIREMENTS MANAGEMENT FINDINGS 54
3.4 FDSH OPERATING ENVIRONMENT FINDINGS 59
3.5 FDSH SOFTWARE DEVELOPMENT FINDINGS 64
3.6 FDSH SYSTEM AND ACCEPTANCE TEST FINDINGS 74
3.7 FDSH DATA MANAGEMENT FINDINGS 79
3.8 FDSH OPERATIONS OVERSIGHT FINDINGS 85

APPENDICES 89

APPENDIX A: ACRONYMS 90

APPENDIX B: INTERVIEWS AND MEETINGS 94

APPENDIX C: REVIEWED DOCUMENTATION 95

APPENDIX D: RISK DETERMINATION 99

D.1 RISK DESCRIPTION 99
D.2 RISK DETERMINATION 99
D.3 RISK MITIGATION AND RECOMMENDATIONS 99

APPENDIX E: FMPS IV&V CODE REVIEW TOOLS 102

APPENDIX F: DETAILED CODE REVIEW FDSH 103

Figures

Figure 1: Total Open Findings..... 1
Figure 2: Findings by Scope of Service Area..... 2
Figure 3: Total Findings by Risk Level..... 3

Tables

Table 1: Findings by Area 2
Table 1.1 FFM No Change from Previous Assessment 6
Table 1.2 FDSH No Change from Previous Assessment 6
Table 2-1 FFM Quality Management Findings..... 8
Table 2-2 FFM Training Findings 11
Table 2-3 FFM Requirements Management Findings 14
Table 2-4 FFM Operating Environment Findings..... 18
Table 2-5 FFM Software Development Findings 20
Table 2-6 FFM System and Acceptance Testing Findings 29
Table 2-7 FFM Data Management Findings 36
Table 2-8 FFM Operations Oversight Findings..... 46
Table 3-1 FDSH Quality Management Findings 49
Table 3-2 FDSH Training Findings 51
Table 3-3 FDSH Requirements Management Findings..... 54
Table 3-4 FDSH Operating Environment Findings 59
Table 3-5 FDSH Software Development Findings..... 64
Table 3-6 FDSH System and Acceptance Test Findings 74
Table 3-7 FDSH Data Management Findings..... 79
Table 3-8 FDSH Operations Oversight Findings 85
Table B-1 Interviews & Meetings 94
Table C-1 Reviewed Documentation 95
Table D-1 Risk Scale and Necessary Actions 99
Table D-2 Probability Assessment Criteria 100
Table D-3 Impact Assessment Criteria 100
Table D-4 Risk Value 101
Table E-1 Code Review Tools 102
Table F-1 Critical Violations Findings FDSH..... 103
Table F-2 Major Violations Findings FDSH..... 105

EXECUTIVE SUMMARY

This report presents the results of the Assessment #10 performed by the Independent Verification & Validation (IV&V) contractor, TurningPoint Global Solutions, which was tasked by the Centers for Medicare and Medicaid Services (CMS) to provide technical audits of the Federal Marketplace Program System (FMPS). The team focused on several specific areas for this assessment for Release 7 and the additional interim releases leading up to October 1, 2013.

Assessments 1 through 9 and 11 through 13 were delivered earlier, and partial corrective action responses have been received from the responsible organizations. The following table depicts the remaining total open findings by organizational responsibility.

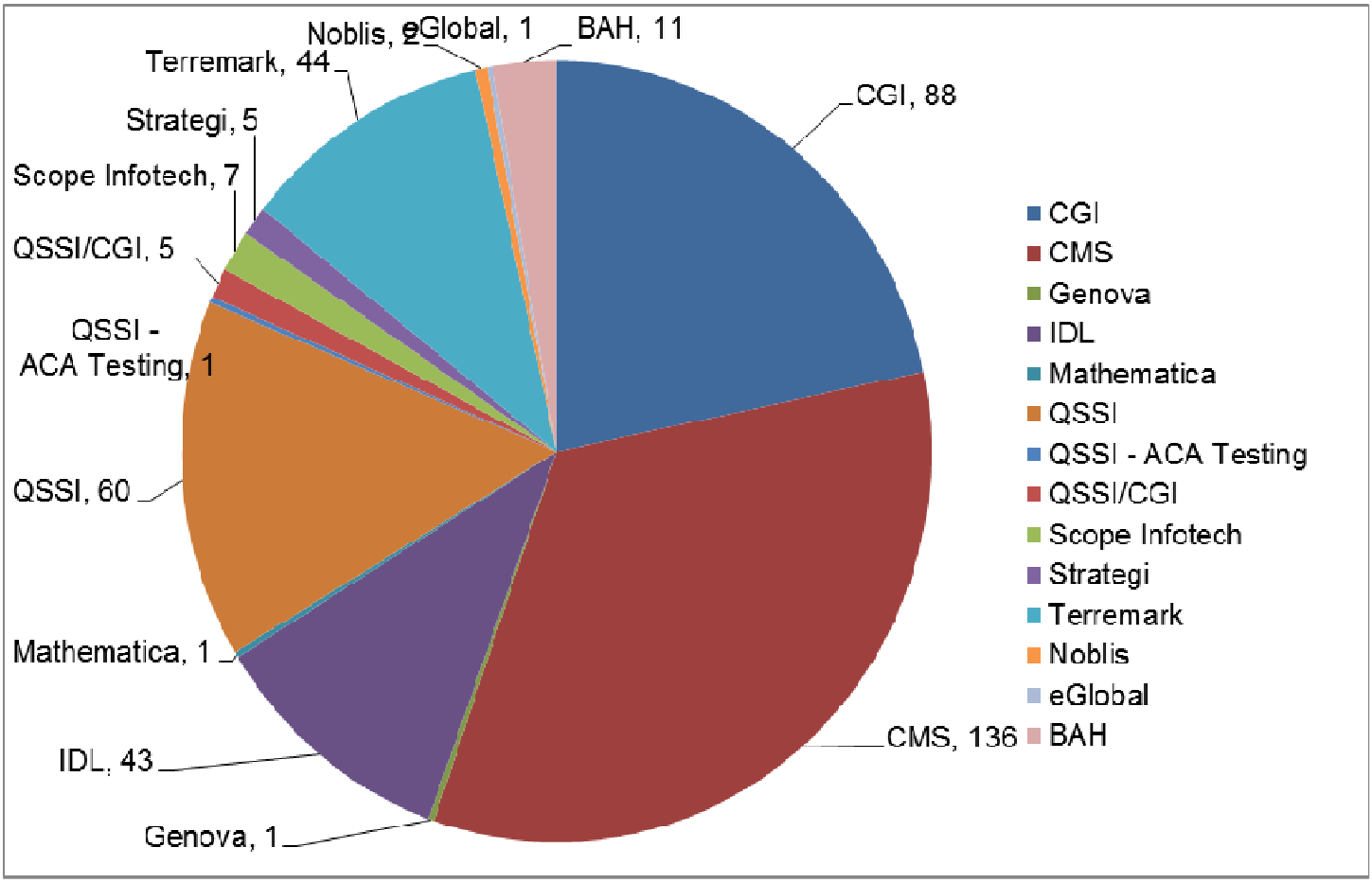


Figure 1: Total Open Findings

This assessment was placed on hold at the request of CMS in order to focus resources on Assessments #11 through #13 due to program priorities. This Assessment was resumed on October 1, 2013.

Table 1 shows the total findings with risk values, by areas for this assessment only.

Table 1: Findings by Area

Total Findings				
Systems	**Low**	**Moderate**	**High**	**Total**
FFM	7	22	26	55
FDSH	3	26	25	54
Total	**10**	**48**	**51**	**109**

Figure 2 displays a summary of findings for this assessment, with a distribution of risk levels. A description of the determination of risk levels appears in Appendix D: Risk Determination.

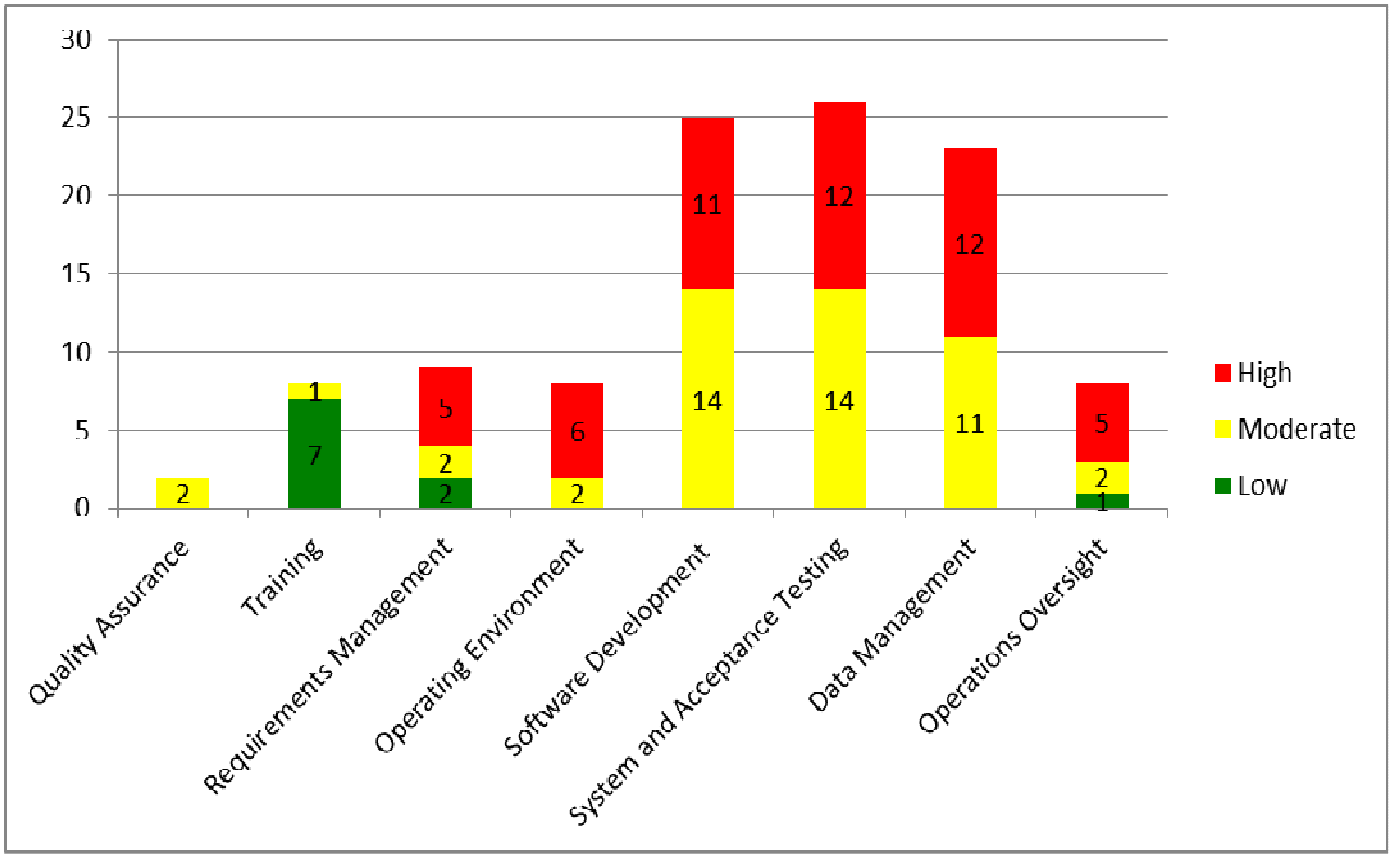


Figure 2: Findings by Scope of Service Area

Figure 3 displays a summary of total findings by risk level.

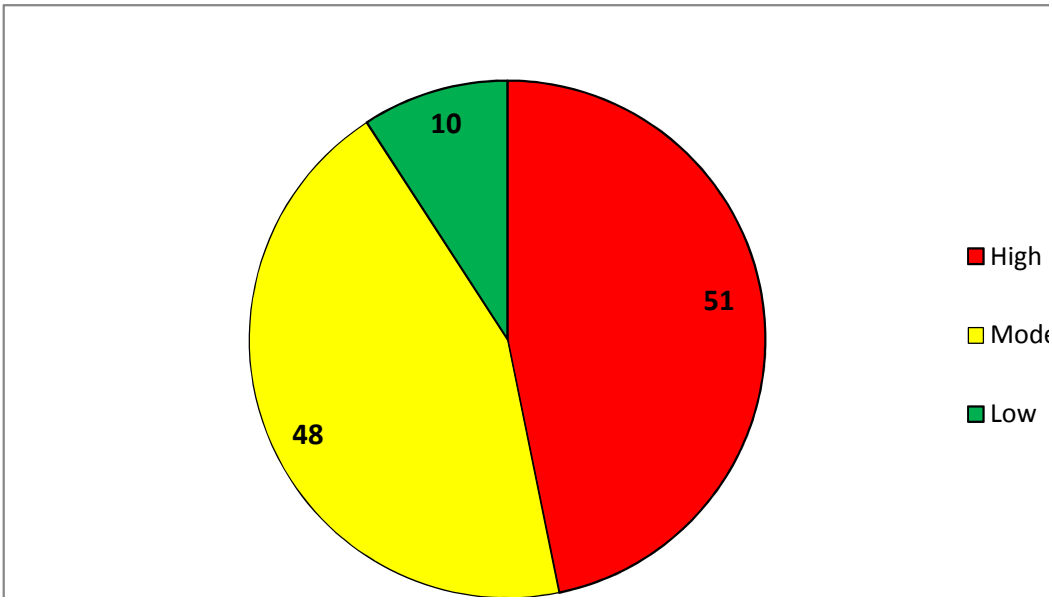


Figure 3: Total Findings by Risk Level

RECOMMENDATIONS

The following are summaries of the recommendations made for each assessment area reviewed:

Requirements Management:

- Ensure that requirements traceability is documented for both forward and backward traceability to ensure that there is management visibility into:
    a. The amount of product completed
    b. The amount of product under development
    c. No product has been developed without a requirement
- Ensure that the status of every user story is accurately updated.
- Ensure that timely secure coding practices are implemented during development, not after application scanning.

Operating Environment:

- Ensure there are performance measurement and end-to-end test plans, test cases and results in CALT for complete stakeholder visibility.
- Establish capacity planning process, procedures and documentation to ensure capacity is adequate.
- Ensure vendor software support documentation and Service Level Agreements (SLAs) are made available for stakeholders.

Software Development:

- Follow Java coding conventions and web optimization techniques; leverage the Sonar tool to review adherence to conventions; conduct rigorous performance testing; and fix all blocker, critical and major source code violations identified by Sonar.
- Ensure all development artifacts are under configuration control.
- Ensure design products address: traceability, availability, accessibility, integrity, performance, reliability, regulations and security.

System and Acceptance Test:

- Reinstate the use of the Testing Playbook; ensure code base, release documentation, test data, environments and schedule are correctly established to support testing during test readiness reviews.
- Evaluate and provide an adequate number of test environments.
- Plan for and provide evidence of performance testing execution for all releases and interfaces for management visibility and to mitigate issues prior to release to production.

Data Management:

- Document the approach and design used in designing the Marklogic database; ensure Data Management Body of Knowledge (DMBOK) best practice areas are covered.
- CMS should establish a RACI (Responsibility, Accountability, Consulted, and Informed) chart which addresses the unique roles and responsibilities for CMS and all the contractors involved in data management activities.
- CMS should establish quality completeness criteria checklists and ensure they are used at all major checkpoints and work product review discussions/approaches or strategies.

Operations Oversight:

- Follow CMS security authorization standards and federal minimum controls (FIPS 200) for disaster recovery.
- Use the Integrated Master Schedule (IMS) to assess the impact of delays and manage the program.

1 INTRODUCTION

1.1 BACKGROUND

The FMPS program was initiated by CMS to provide health insurance marketplace capabilities required by the Patient Protection and Affordable Care Act (PPACA) of 2010. In support of the Federal Marketplace Program System (FMPS) effort, CMS employed TurningPoint to provide an independent and unbiased analysis of the FMPS components and artifacts. CMS tailored the Institute of Electrical and Electronics Engineers (IEEE) 1012 standard to 106 Verification and Validation (V&V) service areas covering the nine Scope of Service areas in the FMPS IV&V Statement of Work (SOW): Quality Management, Training, Requirements Management, Operating Environment, System and Acceptance Testing, Data Management, and Operations Oversight. Not all service areas will be covered in all assessments.

1.2 SCOPE

The scope of this assessment is as follows:

- Documentation related to the Release 7 and the interim releases leading up to October 1, 2013.
- Review and analysis of the FFM and Federal Data Services Hub (FDSH) current code.

1.3 FMPS OVERVIEW

The IV&V team analyzed and organized the assessment of FMPS in the following areas:

- FFM, which is the system that serves the needs of individuals and small businesses within states where those states do not have their own state-run marketplace.
- FDSH, or the Hub, which provides common services and interfaces to federal agency information.

1.4 IV&V APPROACH AND METHODS

Our approach was modified for this assessment from the structured approach. It included: planning the scope of the assessment, requesting pertinent documentation, conducting interviews before August 2013, participating in program meetings, and identifying early warning signs and areas of risk to focus the assessment depth. The IV&V approach to working with federal and contractor organizations is cordial and supportive of priorities, while maintaining independence and objectivity during the assessment.

The IV&V team used CALT to identify the documents and artifacts related to the scope of the assessment during the review of relevant documentation for Assessment 10, items that remain open in the Corrective Action Plan (CAP) from previous assessments were documented and are listed in the tables below:

Table 1.1 FFM No Change from Previous Assessment

IVV Task: RM-1	**No change from Assessment 1, Finding #2 (FFM):** No evidence of mapping of legislation to Blueprints.
	No Change from Assessment 2, Finding #2 (FFM): Process Deviation: There are conflicts among various documents and between documentation and practice regarding which RM process FFE is following and which gate reviews are mandated.
IVV Task: RM-4	**No Change from Assessment 6 Finding #1 (FFM): Completeness**: Division of responsibility for traceability of requirements among the contractors is not clearly defined.
	No Change from Assessment #6 Finding #2 (FFM): Completeness: CMS is not enforcing the requirement management process for traceability.
	No Change from Assessment #6 Finding #7 (FFM): Consistency: Blueprint business process (BP) description is inconsistent
IVV Task: RM-5	**No Change from Assessment 1, Finding 2 (FFM/FDSH):** Blueprints are not baselined and it is not clear that they are under formal configuration control.
IVV Task: RM-9	**No Change from Assessment 8, Finding #1 Correctness:** Asigra tool not upgraded to provide consolidated reports for cloud backups.
	No Change from Assessment 8, Finding # 6 Consistency: Conflicting information regarding weekly backups.

Table 1.2 FDSH No Change from Previous Assessment

IVV Task: RM-1	**No Change from Assessment 2, Finding #2 (FDSH): Completeness:** There is no evidence of procedures describing how Product Backlog is Scoped and sized
	No Change from Assessment 2, Finding #5 (FDSH): Collaboration: There is no evidence that QSSI is using CALT Dashboard to collaborate with stakeholders
	No Change from Assessment 2, Finding #6 (FDSH): Collaboration: It's not clear if QSSI is using burn-down metrics to report on project status in real time and collaborate with stakeholders.
	No change from Assessment 1, Finding #2 (FFM/FDSH): No evidence of mapping of legislation to Blueprints.
IVV Task: RM-4	**No Change from Assessment 2 – Finding #1 (FDSH): Consistency / Traceability:** Unable to establish traceability from Blue Print to user story forward and backward.
	No Change from Assessment 2, Finding #2 (FDSH): Consistency: The RTM is not consistent with the release notes
IVV Task: RM-5	**No Change from Assessment 1, Finding 2 (FFM/FDSH):** Blueprints are not baselined and it is not clear that they are under formal configuration control.
IVV Task: RM-9	**No Change from Assessment 8, Finding # 1 Correctness:** Asigra tool not upgraded to provide consolidated reports for cloud backups.
	No Change from Assessment 8, Finding # 6 Consistency: Conflicting information regarding weekly backups.
IVV Task: ST-1	**No Change: No change since assessment 2 – Consistency:** Unit testing approach not consistent with Agile.
	No Change: No change since assessment 2 – Verifiability: There is no evidence of gate reviews before entering system and acceptance testing.
IVV Task: ST-10	**No Change: No change since assessment 2 – Correctness:** Some interface integration tests performed in developers' environments may not have accounted for CMS environment differences.

The findings are categorized by system and presented in tables. Each finding includes an IEEE categorization, impact statement, sources, risk probability, risk impact, and risk value. Please see Appendix D: Risk Determination for more detailed information about the method used to determine risk impact, probability and value.

Code reviews were performed with the use of Sonar and Sonar plug-ins like JavaScript and Toxicity Chart, Jhawk, JSHint/Rhino tools, as well as manual sampling of the source code. Maintainability determinations were based on several metrics, such as coupling and cohesion. Values are included in the tables in the report.

1.5 ASSUMPTIONS

The IV&V team made the following assumptions during this third assessment:

- CALT/Subversion (SVN) is the only repository of source code for FDSH and FFM.
- CALT contains all of the artifacts involved in all of the assessment areas.
- CMS and contractor staff have provided accurate and current information during interviews, meetings and questionnaires.
- Finding results that were part of assessments carried out while this assessment was on hold are not reported in this assessment.

1.6 CONSTRAINTS

The IV&V team was constrained by the following during this tenth assessment:

- There was limited access to Federal Government and Federal contractor status and technical exchange meetings until July 2013.
- There was no access to test toolsets (HP Quality Center, IQ Suite for instance, to authenticate test results) used by Federal contractors.
- Unable to schedule interviews with contractors due to activity related to production deployment from 10/1/2013.
- Unable to obtain the ACA Testing Documentation.

1.7 REFERENCES

The standards listed below were utilized for the IV&V team's review of the FMPS Program and in the preparation of the Assessment 10.

- IEEE Standard for Software Verification and Validation 1012-2004
- IEEE Recommended Practice for Software Requirements Specifications 830-1998
- IEEE Standard 829/1998 for Software Test Documentation
- The Software Engineering Institute (SEI) Capability Maturity Model Integration (CMMI)
- Project Management Institute's Project Management Body of Knowledge (PMBOK)
- CMS Expedited Lifecycle Process (XLC)
- Section 508 Accessibility of Electronic and Information Technology
- Guidance for Exchange and Medicaid IT Systems, V 1.0 and 2.0
- Medicaid and Exchange IT Architecture Guidance

2 FFM

An in-depth review of the code was performed for FFM, as well as assessments of the documentation received after November 15, 2012. The findings from these assessments are categorized in accordance with the IV&V Scope of Services laid out in the FMPS IV&V Statement of Work (SOW).

2.1 FFM QUALITY MANAGEMENT FINDINGS

Table 2-1 FFM Quality Management Findings

IVV Task: QA-3	**Verify that the QA organization monitors the fidelity of all defined processes in all phases of the project.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Positive Finding**: The Internal QA organization conducts audits for all groups	**N/A**			
Finding Detail	The internal QA group for CGI conducts periodic audits on the software development and testing groups to ensure they are following defined processes and procedures.				
Potential Impact	N/A				
Recommendation	N/A				
Source(s)	**CGI:** QM portal on SharePoint				
IVV Task: QA-4	**Verify that the quality of all products produced by the project is monitored by formal reviews and sign-offs.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Consistency:** The sign-off process is inconsistent.	**4**	**2**	**8**	**Moderate**
Finding Detail	Sign-off of documents in CALT is not consistent some documents do not have sign off/ approval pages. When approval pages are present sign off is not done.				
Potential Impact	If approval is not made then development of unapproved processes may occur impacting customer use and performance				
Recommendation	Ensure that all documentation that requires approval have signatures verified upon delivery.				

Source(s)	**CALT:** doc24022 FEPS-FFE Platform Architecture doc46176: EE_R7.0_SystemDesignDocument				
IVV Task: QA-5	**Verify that project self-evaluations are performed and that measures are continually taken to improve the process.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Positive Finding:** Evaluation an update of internal processes is performed.	**N/A**			
Finding Detail	After each delivery and at lesson learned meeting the internal processes are reviewed and updated as appropriate.				
Potential Impact	N/A				
Recommendation	N/A				
Source(s)	**CGI:** QM portal on SharePoint				
IVV Task: QA-10	**Review and make recommendations on all defined processes and product standards associated with the system development.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Positive Finding:** CGI follows traditional QA product and process standards, including Agile development	**N/A**			
Finding Detail	CGI has developed an internal, proprietary document, Application Lifecycle Management (ALM) Agile Methodologies Health & Compliance Programs (HCP). This document references the 12 Agile principles and maps the project processes to the Agile framework.				
Potential Impact	N/A				
Recommendation	N/A				
Source(s)	**CGI:** QM portal on SharePoint				
IVV Task: QA-11	**Verify that all major development processes are defined and that the defined and approved processes and standards are followed in development.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Positive Finding:** The CGI development group follows detailed and defined processes.	**N/A**			
Finding Detail	Processes and procedures for the development group are defined and followed as evidenced by QA Audits.				
Potential Impact	N/A				
Recommendation	N/A				
Source(s)	**CGI:** QM portal on SharePoint				
IVV Task: QA-13	**Verify that all process definitions and standards are complete, clear, up-to-date, consistent in format, and easily available to project personnel.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**

Finding 1	**Positive Finding:** Internal processes and procedures follow a standard format and are available to all users	**N/A**
Finding Detail	Internal processes and procedures follow a standard format and are available to all users working in the development group.	
Potential Impact	N/A	
Recommendation	N/A	
Source(s)	**CGI:** QM portal on SharePoint	

2.2 FFM TRAINING FINDINGS

Table 2-2 FFM Training Findings

IVV Task: TR-1	Review and make recommendations on the training provided to system users. Verify sufficient knowledge transfer for maintenance and operation of the new system.	Prob (P)	Impact (I)	Risk Score (P x I)	Risk Level
Finding 1	**Verifiability:** No evidence found for system training taking place in CALT.	**2**	**2**	**4**	**Low**
Finding Detail	User guides exist and are well maintained; however, there is no evidence found in CALT to indicate that system training is happening.				
Potential Impact	If training is not provided to the system users, then the users will not have adequate knowledge on how to use the system.				
Recommendation	Put the system training in CALT.				
Source(s)	**CALT:** doc51976 EE_R7.0.1_UserGuide				
IVV Task: TR-1		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 2	**Positive Finding:** CIBER-Arch train the trainer session held on 8/20/2013	N/A			
Finding Detail	On the 8:00 AM Daily Morning Production Support Status Call it was stated that train the trainer for CIBER-Arch is schedule for 8/20/2013.				
Potential Impact	N/A				
Recommendation	N/A				
Source(s)	**Meeting:** 8:00 AM Daily Morning Production Support Status Call				
IVV Task: TR-1		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 3	**Completeness:** Additional details would make Tivoli Workload Scheduler (TWS) training guide more comprehensive	5	1	5	**Low**
Finding Detail	Users being trained with the TWS training guide would benefit from additional details in the training guide. The user training guide was well designed; however, the level of detail would require a user to have existing knowledge of TWS prior to the training.				
Potential Impact	If adequate detail is not provided with the training material then a risk may occur that the training recipient my not receive the necessary knowledge needed to use TWS tool and training guide was not provide good reference material after the training.				
Recommendation	Update the TWS training guide with additional details assuming that the user being trained has no prior knowledge of TWS.				

Source(s)	**CALT:** doc28140 Tivoli Workload Scheduler (TWS) training 1				
IVV Task: TR-4	**Verify that all necessary policy and process and documentation is easily available to users.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Readability:** Numerous spelling errors in the text describing screen function in user guides.	**5**	**1**	**5**	**Low**
Finding Detail	There are 46 spelling errors in the text describing the screen function in the user guides that were updated for release 7. This may indicate a review was not performed.				
Potential Impact	If spelling errors are present in the documents, then it may be misinterpreted by a user of the document.				
Recommendation	Perform a review of the user guide documents and correct text prior to publishing in CALT.				
Source(s)	**CALT:** doc51976 EE_R7.0.1_UserGuide				
IVV Task: TR-4		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 2	**Completeness:** Additional details would make the TWS training guide more comprehensive	**5**	**1**	**5**	**Low**
Finding Detail	Users being trained with the TWS training guide would benefit from additional details in the training guide. The user training guide was well designed; however, the level of detail would require a user to have existing knowledge of TWS prior to the training. For example: • Roles and responsibilities are not defined. • User guide does not show how to access the system, such as signing on. • There are references different features of the tool, such as 'variables' and 'job recovery option,' but there is no guidance or examples of how to use the features				
Potential Impact	If adequate detail is not provided with the training material then a risk may occur that the training recipient my not receive the necessary knowledge needed to use TWS tool and training guide was not provide good reference material after the training.				
Recommendation	Update the TWS training guide with additional details assuming that the user being trained has no prior knowledge of TWS.				
Source(s)	**CALT:** doc28140 Tivoli Workload Scheduler (TWS) training 1				
IVV Task: TR-4		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 3	**Positive Finding:** Policies referenced in PM_R6_RatingModule_UserGuide (doc33123)	**N/A**			
Finding Detail	Section 2 of Doc33123 reference the Consumer Information & Insurance Oversight (CCIIO) site http://cciio.cms.gov/programs/exchanges/qhp.html for the user to obtain information regarding specific policy and submission criteria for each section of the Rating Module.				
Potential Impact	N/A				

Recommendation	N/A				
Source(s)	**CALT:** doc33123 PM_R6_RatingModule_UserGuide				
IVV Task: TR-4		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 4	**Completeness:** User Guide (doc33123) does not contain revision history table and it is a version 5.	**5**	**1**	**5**	**Low**
Finding Detail	Doc33123 does not contain a revision history table to inform the user of changes to the document				
Potential Impact	If the document does not contain a revision history table, then the user may be unable to understand changes to a document.				
Recommendation	Add version table to the document to ensure it is clear as to when and what changes were made to the document.				
Source(s)	**CALT:** doc33123 PM_R6_RatingModule_UserGuide				

2.3 FFM REQUIREMENTS MANAGEMENT FINDINGS

Table 2-3 FFM Requirements Management Findings

IVV Task: RM-4	Verify that software requirements can be traced through design, code and test phases to verify that the system performs as intended and contains no unnecessary software elements.	Prob (P)	Impact (I)	Risk Score (P x I)	Risk Level
Finding 1	**Consistency:** User Stories, Business Service Definitions (BSD), Business Service Specifications (BSS) and Data Service Specifications (DSS) do not provide sufficient details.	**4**	**4**	**16**	**High**
Finding Detail	Review of documentation indicated the following: • User Story status marked as "in progress". • User story titles and narratives were one and the same or didn't have enough information to develop success criteria for testing, status denoted as "in progress", and not assigned to anyone. • BSDs, BSSs, and DSSs were missing information or marked as To Be Determined (TBD) for security, "Quality of Service" was missing and/or core business mapping missing. • Majority of the BSDs and Service Specs in Requirements Traceability Matrix (RTM) were marked with a status of "to be updated". All had a status of "DRAFT" in CALT.				
Potential Impact	If User Stories, BSDs, BSSs and DSSs do not provide sufficient details, then the program may be unable to develop and/or update service specifications (BSDs, BSSs, DSSs, User Interface (UI) Diagrams, UI Service Specs) with the accuracy and traceability necessary to comprehensively define, plan and execute test cases which may impact the quality of the 8/30 release.				
Recommendation	The recommendations for this finding are: • Ensure that descriptions provide sufficient detail to develop and create other documentation during the Software Development Life Cycle (e.g. test cases). • Ensure that all documents are completed for items that are “TBD”, “In progress”, or “DRAFT” by implementation date.				

Source(s)	**CALT**: doc46152 EE_R7.0_SRD_RTM_Draft doc46005 EE_R7.0_BusinessServiceSpecifications doc46006 EE_R7.0_DataServiceSpecifications doc46008 EE_R7.0_ServiceSequenceDiagrams artf150336 artf150342 artf96183 artf149831 thru 149835 artf151100 thru 151120 artf151047 thru 151073 artf151089 thru 151099				
IVV Task: RM-4		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 2	**Consistency & Completeness:** There is a lack of traceability between Release Plans and Build/Release Notes, Service Specifications, UI Specifications, and the RTM.	**4**	**5**	**20**	**High**
Finding Detail	Review of documentation indicated the following: • Lack of traceability to BSDs, Service Specifications, Service Sequence Diagrams, and UI Specifications. Requirements in RTM indicated these as "to be updated" and therefore could not be traced. • While traceability to the development backlog was provided, a significant number of development backlog items were not assigned to an individual or team. • Status of "approved" but not assigned to any individual or team. • Development Backlog indicated testing in progress while user stories and business service definitions were incomplete.				
Potential Impact	If traceability is inconsistent, then: • As a result it will be difficult to trace development activities to resources responsible for creating code/scripts/program logic etc.., perform test case reviews and resolve defects. • The program may be unable to develop and/or update service specifications (BSDs, BSSs, DSS, UI Diagrams, UI Service Specs) with the accuracy and traceability necessary to comprehensively define, plan and execute test cases which may impact the quality of the 8/30 release.				

Recommendation	Recommendations for this finding are: • CMS should ensure the traceability process is documented. • Ensure responsibilities regarding all requirements documents traceability are understood and adhered to by all contractors. • Ensure Contractor traceability deliverables are complete at quality reviews. • Ensure that responsibility for maintaining traceability across all releases is understood and maintained by all contractors. • Ensure consistent traceability across the FMPS requirement. • Choose appropriate method for tracing user stories. • Build an automated traceability report to run on demand and include an option of listing all or selected parts of the requirement hierarchy. • Extract each requirements element from CALT for testing to ensure that it is related to other requirement elements. • Automate the tracing of software requirements across design, code and test phases. • Ensure that in a given sprint, the status of every User Story implemented in this sprint has a status of "Development Completed". For User Stories not implemented the status indicative of the upcoming sprint release should be displayed. Likewise, assure that the status of every related requirement element (Business Services through Development Tasks) is closed or completed.
Source(s)	**CALT:** doc46152 EE_R7.0_SRD_RTM_Draft doc46153 EE_R7.0_ReleasePlan doc46005 EE_R7.0_BusinessServiceSpecifications Touching Bases--delayed opening for students doc46012 EE_R7.0_UISpecifications artf150336 artf150342 artf96183 artf149831 thru 149835 artf151100 thru 151120 artf151047 thru 151073 artf151089 thru 151099

IVV Task: RM-9		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Verifiability:** Duplicate documents in CALT may confuse the user as to processes & procedures Backup and Restore Services procedures (doc12881) and ECloud Backup Process Document 05_08_2012 (doc7475).	**5**	**1**	**5**	**Low**
Finding Detail	Documents doc12881 "Backup and Restore Services procedures" dated October 9, 2012 and doc7475 "ECloud Backup Process Document 05_08_2012" dated May 17, 2012 contain identical information but have different file names in CALT.				
Potential Impact	If duplicate documents exist in CALT then, confusion and schedule impacts may occur if updates are made to one of the documents and the other document is referenced by the user.				
Recommendation	Determine which document should be retained in CALT and delete the duplicate document.				

Source(s)	CALT: doc7475 ECloud Backup Process Document 05_08_2012 doc12881 Backup and Restore Services procedures doc12885 OM Manual eCAP

2.4 FFM OPERATING ENVIRONMENT FINDINGS

Table 2-4 FFM Operating Environment Findings

IVV Task: OE-1	**Evaluate new and existing system hardware configurations to determine if their performance is adequate to meet existing and proposed system requirements.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Completeness –** Performance Measurement Plan is incomplete.	**5**	**3**	**15**	**High**
Finding Detail	Performance measure plan is out dated, last updated in January 2012. Methodology and algorithms are not defined and described clearly in performance measurement plan.				
Potential Impact	If there is no proper measurement and planning for the performance of system, then it will be hard to determine what is needed for the system to be available at peak volumes/traffic.				
Recommendation	Update the doc4383 FFE PerformanceMeasurementPlan document with adequate information in each section. Include the tools used for measuring and reporting the performance.				
Source(s)	**CALT:** doc4383 FFE PerformanceMeasurementPlan doc24022 FFE12-002 FMPS-FFE Platform Architecture (1)				
IVV Task: OE-9	**Evaluate any current and projected vendor support of the software, as well as the CMS software acquisition plans and procedures.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Verifiability:** Unable to verify current and projected vendor software support.	**5**	**2**	**10**	**Moderate**
Finding Detail	There was no evidence located in CALT on SLA or any other type of documentation detailing vendor software support. We found evidence of list of installed software and approved applications but found no evidence of the level of vendor support. Here's a partial list of some of the software: Oracle 11gR2, Statistical Analysis System (SAS) Windows Clients 9.3, Citrix XenApp Server 6.5, Citrix Data Collector 6.5, Structured Query Language (SQL) Server 2008 R2 SP1, MarkLogic 5.0,2, Apache 2.2.15, Drupal 7.12, Sugar CRM 6.3.1, Informatica, Cognos etc.				
Potential Impact	If vendor software support is not readily documented and available, then this could impact timely support and resolution on software issues.				
Recommendation	Vendor software support documentation and SLA should be made available in a centralized location and process put in place to review annually.				

Source(s)	**CALT:** doc12880 PaaS VM Software Components doc12381 FFE_HTD doc11023 CSP4IaaS C&A Artifacts Update 091212				
IVV Task: OE-12	**Evaluate the results of any volume testing or stress testing.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Verifiability** – Unable to find the Volume and stress testing metrics in CALT.	**5**	**5**	**25**	**High**
Finding Detail	There are no artifacts for volume and stress testing in CALT.				
Potential Impact	If there is no posted volume and stress testing results, then IV&V cannot provide visibility of the quality to upper management.				

Recommendation	Provide the testing results in CALT. Verify that the results of volume and stress testing will meet nonfunctional performance requirements.
	
	Expectations of performance, load and stress testing include:
	• Develop a workable strategy for performance testing an application/system
	  ○ An analysis of the situation/performance test scenario and understanding the planning and design issues associated with performance testing and how it relates to the development process
	  ○ Understanding the goal - validate the performance test project need and feasibility
	• Assessing infrastructure issues - learn how to deal with environment and architecture issues
	  ○ What must be part of the test; target platform and systems; network configuration; scalability and extrapolation
	• Designing the test – Define operational profiles and load definitions; understand and select the various types of performance tests
	  ○ Define the workload – Operations Profile; transactions to be simulated; analyze factors affecting the load definition; calculate load characteristics
	• Specific tuning recommendations; problem analysis, debugging; tools usage
	  ○ Refining measurements; response times, resource usage, etc.
	  ○ Assist the technical team after tuning and debugging
	• Reporting performance test results
	Present conclusions and recommendations; Assessment issues				

Source(s)	**CALT:** No Documentation Found				

2.5 FFM SOFTWARE DEVELOPMENT FINDINGS

Table 2-5 FFM Software Development Findings

IVV Task: SD-2	Evaluated the design products for adherence to the project design methodology and standards.	Prob (P)	Impact (I)	Risk Score (P x I)	Risk Level
Finding 1	**Positive Finding:** CGI leverages most of the CMS software development tools.	**N/A**			
Finding Detail	AndroMDA is used as the model driven architecture framework to generate code from the Unified Modeling Language (UML) models. MagicDraw is used for creating UML models. Collaborative Application Lifecycle Tool (CALT) of TeamForge is used too as the Application Lifecycle Management (ALM) tool which included subversion for source code management. Automatic build management and continuous integration tools including Jenkins, Sonar, and Nexus etc. are used to manage the entire software lifecycle from development to production. CALT is used as the centralized repositories for all project artifacts, including source code and file releases. Agile Methodology is used for software development.				
Potential Impact	N/A				
Recommendation	N/A				
Source(s)	**CALT/SVN:**				
IVV Task: SD-4	**Verify that design requirements can be traced back to system requirements.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Traceability:** Not all the designs can be traced back to the system requirements in CALT.	**4**	**3**	**12**	**Moderate**
Finding Detail	The following Technical Design Documents and BSDs do not have any reference to user stories or CALT artifacts: doc51961, doc51919, doc51954.				
Potential Impact	If design documents cannot be traced back to system requirements, then there may be functionality that is not required.				
Recommendation	Ensure that Technical Design Documents and BSDs have proper reference to user stories and CALT artifacts.				
Source(s)	**CALT:** doc51919 EE_R7.0.1_SystemDesignDocument.docx doc51961 EE_R7.0.1_BSD.zip doc51954 EE_R7.0.1_UISpecifications.zip				
IVV Task: SD-4		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**

Finding 2	**Completeness:** Some design documents have missing information.	**4**	**3**	**12**	**Moderate**
Finding Detail	Review of documentation indicated: • BSDs, BSSs, and DSSs were missing information or marked as "TBD" for security, "Performance Measures ", and "Quality of Service" was missing and core business mapping was missing. (doc51961-CBS-EXCH-EE-07) • Business Service Specifications (BSSs) did not have module name, implementation elements and "TBD" for functional requirement. (doc51888 - EE_BenefitEnrollmentProcessing_BusinessServiceSpecification.docx)				
Potential Impact	If design documents incomplete, then there may be functionality missing which will impact quality.				
Recommendation	• Ensure that descriptions provide sufficient detail to develop and create other documentation during the Software Development Life Cycle (e.g. test cases). • Ensure that all documents are created for all instances so that "TBD", "In progress", or "DRAFT" is not denoted by implementation date.				
Source(s)	**CALT:** doc51919 EE_R7.0.1_SystemDesignDocument.docx doc51961 EE_R7.0.1_BSD.zip doc51954 EE_R7.0.1_UISpecifications.zip doc51888 EE_R7.0.1_BusinessServiceSpecifications.zip				
IVV Task: SD-6	**Perform an evaluation and make recommendations on existing job control and on the process for designing job control.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Completeness:** There are multiple documents without detailed job control processes.	**4**	**3**	**12**	**Moderate**
Finding Detail	Design of the specific jobs and job control are not documented. • EE, Plan Management (PM), and Quality Management (QM) Software Design Document (SDDs) contain this wording: ""Batch specifications for the (EE/PM) module will be included in subsequent releases." The QM SDD contains an empty table of Batch Specifications (In doc 12497 for Release 3) • EE Release 7 System Design Document (doc51919 and doc55478) does not address any Batch specifications. But there is description of used batch job. In doc51919 p59 there is "Sequence diagrams describing the ExpireFiveYearBar batch job" in Table 6: Service Sequence Diagram Document Mapping. In doc51919 p27 in Scenario 1: Scanned English document, there is batchID used. But no details provided on where the batch job is and how it is executed.				
Potential Impact	If all the batch jobs do not include all of the details, then it may not be possible to schedule the jobs and this may affect the system performance or cause failure or timeout issues.				

Recommendation	Document the following details for all batch jobs: • User Story Covered in the Batch Specification • Batch Name and Description • Batch Parameters, Filters, and Variables • Batch Operational Capabilities (including Job Partitioning, Job Control, Transaction Control, Restart/Resume, and Chaining) • Batch Processing				
Source(s)	**CALT:** doc12497 QM_R3S9_SystemDesignDocument.doc doc10615 EE_R3_SystemDesignDocument.docx doc12464 PM_R3S9_SystemDesignDocument.docx doc55478 EE_R7.0.2_SystemDesignDocument.docx doc51919 EE_R7.0.1_SystemDesignDocument.docx				
IVV Task: SD-8	**Evaluate batch jobs for appropriate scheduling, timing and internal and external dependencies.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Verifiability:** IV&V team was unable to verify the batch jobs for appropriate scheduling, timing and internal and external dependencies for Release 7 because this is not documented.	**2**	**4**	**8**	**Moderate**
Finding Detail	There are no documents found in CALT for any batch jobs that related to the software development, so this SOW cannot be verified.				
Potential Impact	If no batch jobs can be evaluated, then there are risks that production applications using batch jobs (doc51919 and doc55478) may contain defects that were not detected prior to implementation.				
Recommendation	Upload documents or scripts for batch jobs into CALT for evaluation.				
Source(s)	**CALT:** doc55478 EE_R7.0.2_SystemDesignDocument.docx, doc51919 EE_R7.0.1_SystemDesignDocument.docx				
IVV Task: SD-9	**Evaluate the appropriate use of OS scheduling software.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Positive Finding**: Quartz open source job scheduling library is used for job scheduling.	**N/A**			
Finding Detail	Quartz open source is licensed under the Apache license, so it has third-party support and it does not need to be customized per the CMS Technical Reference Architecture (TRA). Quartz is also using Cron, which is reliable Unix software.				
Potential Impact	N/A				
Recommendation	N/A				

Source(s)	**CALT:** config/trunk/ffeprops/Private_Cloud_props/tmk-intva-1__FFE_TEST2.Sprint/ffe.properties_data /ec-scripts/trunk/etc/es/crontab /config/trunk/ffeprops/ffx/ee.batch.properties ff/trunk/fm/branches/feature-6.0/fm-business-svcs/esb /src/main/resources/quartz.properties /ff/trunk/fm/branches/feature-6.0/fm-business-svcs/esb/pom.xml /ff/trunk/fm/branches/feature-6.0/fm-business-svcs/esb/src/main/java/gov/hhs/cms/ff/fm/services/business/processinitiation/helpers/ProcessInitiationSchedulerFactory.java				
IVV Task: SD-10	**Verify that job control language scripts are under an appropriate level of configuration control.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Verifiability:** IV&V team is unable to verify that all Job control scripts are under CALT SVN.	**4**	**3**	**12**	**Moderate**
Finding Detail	Even though some of the scripts/configuration are found without proper documentation, it is not evident if all the job control scripts are under configuration control.				
Potential Impact	If the batch jobs are not properly documented and the job control scripts are not under appropriate configuration control, then it may not be possible to evaluate if the jobs are scheduled properly.				
Recommendation	1. Ensure schedule, timing and dependencies of all the batch jobs are well documented. 2. Ensure all the job control scripts are under configuration control.				
Source(s)	**CALT:** gov.hhs.cms.ffe.ee.batch.schedule ffe/trunk/ee/trunk/ee-batch/src/main/resources/META-INF/spring/batch/servlet/override/service-context.xml ffe/trunk/ee/trunk/ee-batch/src/main/resources/META-INF/spring/batch/jobs/reverifyLawfulPresence-job.xml				
IVV Task: SD-11	**Evaluate and make recommendations on the standards and process currently in place for code development.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Process Improvement:** Code development process needs major improvements.	**3**	**4**	**12**	**Moderate**
Finding Detail	There is no evidence of code reviews in CALT. There is no evidence of code quality checks and steps taken to correct Sonar violations.				
Potential Impact	If there is a lack of code reviews and process to follow standards, then it may lead to inefficient and buggy code increasing maintenance costs and application errors that are costly.				
Recommendation	Include peer reviews in the code development process and train developers to follow best coding practices. Use the Sonar tool to document code reviews.				
Source(s)	CALT doc50758 Daily CGI IQ Defect Tracker Extract 09092013 sheet TP_Root_cause_in_Model				

IVV Task: SD-12	Evaluate the existing code base for portability and maintainability, taking software metrics including but not limited to modularity, complexity and source and object size.	Prob (P)	Impact (I)	Risk Score (P x I)	Risk Level
Finding 1	**Correctness:** Too many coding issues and bugs exist in the FFM software.	**4**	**4**	**16**	**High**
Finding Detail	Coding issues/bugs found: • Too many javascripts included in each web page. • Not loading the images first before Java scripts and not including javascripts at the end of Hyper Text Markup Language (HTML) file to make the site more responsive. • Code not handling unavailability of external services with a backup mechanism (e.g- blank security questions issue). • Too many requests to the server.				
Potential Impact	If there are too many bugs and issues in coding, then there may be poor performance and application errors. This will ultimately affect the user experience.				
Recommendation	Follow standard design patterns and efficient coding practices (http://www.oracle.com/technetwork/java/codeconv-138413.html, http://www.oracle.com/us/technologies/java/overview/index.html). Enforce a strict code review process and quality checks to ensure all developers follow the best practices.				
Source(s)	**CALT/SVN:** ffe/trunk/ee/trunk/ee-ui/web/src/main/webapp/auth/ui/individualApplication ffe/trunk/ee/trunk/ee-ui/web/src/main/webapp/auth/ui/myAccount/HTMLViews ffe/trunk/ee/trunk/ee-ui/web/src/main/webapp/js ffe/trunk/ee/trunk/ee-ui/web/src/main/webapp/layout				
IVV Task: SD-12		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 2	**Correctness:** Website optimization techniques are not followed (caching, not compressing java script files, not combining all the files into one)	**4**	**4**	**16**	**High**
Finding Detail	Website Optimization techniques are not being used, e.g., caching, not compressing java script files, not combining all the files into one. Evidence of this is demonstrated by the following errors identified while using Chrome development tools by the IV&V team: • Web pages are not cached properly to improve the performance. • Java script files are not compressed are combined to improve performance. • Loading of the static images on web pages is not optimized				
Potential Impact	If these optimization techniques are not used, then the application may perform poorly and affect the user experience.				

Recommendation	Take steps to ensure website is optimized for performance. Conduct rigorous performance testing of the optimization techniques as there is no single best solution for optimization. • Make sure all the web pages are cached according to the content of the page. This means web pages that do not change often and that do not contain user-specific content should be cached for longer duration. • Make sure static images are cached. • Compress java script files and combine all script files into one (http://betterexplained.com/articles/speed-up-your-javascript-load-time/). • Always test the loading time for each page. • Ensure geographical distribution of server content when using of Akamai Content Delivery Network (CDN) to improve the loading of web pages. • Evaluate the Akamai CDN for performance metrics. • Optimize the loading of static images on web pages.				
Source(s)	**CAT/SVN:** ffe/trunk/ee/trunk/ee-ui/web/src/main/webapp/auth/ui/individualApplication ffe/trunk/ee/trunk/ee-ui/web/src/main/webapp/auth/ui/myAccount/HTMLViews ffe/trunk/ee/trunk/ee-ui/web/src/main/webapp/js ffe/trunk/ee/trunk/ee-ui/web/src/main/webapp/layout				
IVV Task: SD-12		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 3	**Correctness:** Fortify Security Report for Health Insurance Exchange (HIX) shows many security violations.	**4**	**4**	**16**	**High**
Finding Detail	Issues found: • Cross-Site Request Forgery • JavaScript Hijacking: Vulnerable Framework • Poor Error Handling: Overly Broad Catch, • Poor Error Handling: Throw Inside Finally • J2EE Misconfiguration: Excessive Session Timeout • Password Management: Password in Comment • J2EE Bad Practices: Leftover Debug Code • Denial of Service • Dynamic Code Evaluation: Code Injection, • Session Not Invalidated After Logout • Cross-Site Scripting				
Potential Impact	If it is possible to steal or manipulate customer sessions and cookies, then it may be used by a hacker to impersonate a legitimate user who can view or alter user records, and to perform transactions as that user.				

Recommendation	Follow secure coding practices. Fix security issues before CMS independent contractor performs the SCA. Invalidate relevant session identifiers when a user signs out.				
Source(s)	**CALT:** doc22926 UT-Branch_-_Fortify_Security_Report-Final.pdf doc45098-AppScan-FFM.pdf				
IVV Task: SD-15	**Verify that developed code is kept under appropriate configuration control and is easily accessible by developers.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Positive Finding:** FFM codes are checked in at CALT, and under configuration control, and can be accessed easily by developer.	**N/A**			
Finding Detail	FFM codes are checked in at CALT, and under configuration control, there are revision numbers, age, and author for each files. Code can be downloaded by any authorized developer. Please see the diagram below: Project: CMS Exchange Business Requirements Project Home · Tracker · Documents · Tasks · Source Code · Discussions · Reports · File Releases · Wiki [feps_ffe] /				

File	Rev.	Age	Author	Last log entry
[redacted]	118571	30 minutes	[redacted]	Tagged by CI Build # CI_110113_18
	90299	2 weeks		
	44096	6 months		Tag for Sprint 16 baseline.
	50487	3 months		mmorad - EE prime tagged build - EE-PRIME-20130702
	15222	14 months		Modified By: Mansi Changes: Changed reference types to plain strings: referr...
	29998	9 months		Changed folder name to . notation
	118576	26 minutes		Most recent update of Golden Reference List dated 11/01/2013 @ 1:42 PM.
	118536	83 minutes		modified test script for jenkins to email fail buil
	58712	2 months		added the distribution Management section

Potential Impact	N/A				
Recommendation	N/A				
Source(s)	**CALT:** Project: CMS Exchange Business Requirements				
IVV Task: SD-17	**Evaluate the plans, requirements, environment, tools, and procedures used for unit testing system modules.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**

Finding 1	**Verifiability:** No evidence was found of unit testing plan, requirements, environment, tools, procedures, and results for release 7.	3	4	12	**Moderate**
Finding Detail	No evidence of unit testing plans, requirements, environment, tools, procedures, and results were found in CALT for release 7 for the FFM. Only some artifacts found in CALT for unit testing and the statuses are still open (as of Nov 1, 2013): for example: artf148174, artf148184, artf148194, artf148204, artf148214, artf147827. They are Development Tasks and their titles include service code (w/ unit test, ref data gen).				
Potential Impact	If unit testing plans, requirements, environment, tools, procedures, and results are not found in CALT, then the appropriate level of testing may not be verified for the release. This includes verifying traceability to the functions being developed.				
Recommendation	Provide unit testing plan, requirements, environment, tools, procedures, and results for release 7 in CALT for review.				
Source(s)	**CALT:** artf148174 artf148184 artf148194 artf148204 artf148214 artf147827				
IVV Task: SD-18	**Evaluate the level of test automation, interactive testing and interactive debugging available in the test environment.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Correctness:** Level of test automation is low per evidence in CALT.	3	4	12	**Moderate**

Finding Detail	The following files were evaluated. Only EE Test Cases Set 6.xls has one test that is automated using the cron job. In this file there are total 385 tests. Only one test automated. That is 0.23% of automation for this one file. There are no automated tests detected in the other 5 files. EE Test Cases Set 1.xls EE Test Cases Set 2.xls EE Test Cases Set 3.xls EE Test Cases Set 4.xls EE Test Cases Set 5.xls EE Test Cases Set 6.xls

	A	B	C	D	E	F	G	H	I
1	TEST_ID	TESTNAME	D	T	PF	STEP	STEP_DESCRIP	EXPECTED_RESULT	EXEC_S T
671	31825	EE_Automated file Processing of Inbound 834 (Eff_Cancel_term)				Step 1	Login to Putty an	Putty is opened.	Failed
672	31825	EE_Automated file Processing of Inbound 834 (Eff_Cancel_term)				Step 2	Verify 834 file received from	834 is available in the public folder	Failed
673	31825	EE_Automated file Processing of Inbound 834 (Eff_Cancel_term)				Step 3	Automated cron j	Cron job is automated.	Failed
674	31825	EE_Automated file Processing of Inbound 834 (Eff_Cancel_term)				Step 4	Verify once the s	834 file is moved to Private folder.	Failed
675	31825	EE_Automated file Processing of Inbound 834 (Eff_Cancel_term)				Step 5	834 should be located in	File Transfer is successfully done by cron job.	Failed

Potential Impact	If the level of test automation is low, then the regression testing process may be inefficient, and there may be human errors during testing, affecting the quality of the production application.
Recommendation	Automate the testing to minimize the cost and labor for regression testing.
Source(s)	**CALT:** doc49292 EE_R7.0_TestCases.zip

2.6 FFM SYSTEM AND ACCEPTANCE TESTING FINDINGS

Table 2-6 FFM System and Acceptance Testing Findings

IVV Task: ST-1	**Evaluate the plans, requirements, environment, tools, and procedures used for integration testing of system modules.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Completeness:** The Requirements Traceability Matrix (RTM) document for the September 6, 2013 Eligibility & Enrollment (E&E) delivery does not include adequate information to perform forwards and backwards traceability from user stories to test cases.	**5**	**3**	**15**	**High**
Finding Detail	In doc50521 test cases and other data elements in the spreadsheetsuch as business services specification and UI specification are not completed and in the RTM, it is stated that it needs to be updated.				
Potential Impact	If the RTM is not adequately updated then it is difficult to trace the test coverage for the release requirements.				
Recommendation	Update the RTM for the September 6, 2013 delivery to reflect the test cases that are used to provide test coverage for release requirements.				
Source(s)	**CALT:** doc50521 EE_R7.0_SRD_RTM_Draft				
IVV Task: ST-1		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 2	**Completeness:** Test environments not adequately documented and do not mirror production sufficiently for a valid test. Meeting participants indicate confusion about the test environment.	**5**	**5**	**25**	**High**
Finding Detail	Through the "Daily FMPS and Testing Touch Bases Call" and "FMPS (Prod-Dev-Testing) Meeting," it was indicated that the test environments were not adequately provisioned with correct data and code base at almost every release.				
Potential Impact	If test environments are not correctly provisioned then valid testing will not be performed and test results may not be valid.				
Recommendation	Ensure code base, test data and environments are correctly documented and ready to support testing. Reinstate the use of the testing playbook and appropriately update the playbook to provide clear direction regarding code base, test data and environments.				
Source(s)	**Meetings:** Daily FMPS and Testing Touch Base – August 14, 2013; October 3, 2013 FMPS (Prod-Dev-Testing) Meeting – September 13 & 17, 2013				

IVV Task: ST-1		Prob (P)	Impact (I)	Risk Score (P x I)	Risk Level
Finding 3	**Completeness:** Test completeness is affected by the incompleteness of the user stories in the RTM.	**4**	**4**	**16**	**High**
Finding Detail	In doc50521 users stories for September 6, 2013 delivery still show a status of in progress a month after the implementation date.				
Potential Impact	If user stories are not accurately updated, then there is a risk that test cases will be incomplete and incorrect, and therefore the product may be deployed with defects. This may affect maintainability as well.				
Recommendation	Update the user story appropriately to ensure the users stories are addressed through testing.				
Source(s)	**CALT:** doc50521 EE_R7.0_SRD_RTM_Draft				
IVV Task: ST-2	**Evaluate the level of automation and the availability of the system test environment.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Completeness:** Shortage of test environments to adequately test the various releases.	**5**	**5**	**25**	**High**
Finding Detail	There was a lack of planning and management of the test environments. It became apparent to the IV&V Team, while listening to the testing touch base calls, that more test environments would have greatly assisted the testing of code to ensure more complete testing.				
Potential Impact	If a project of this magnitude lacks available test environments, then there may not be sufficient time code to adequately test code before the code was promoted to successive environments.				
Recommendation	Evaluate and provide an adequate number of test environments.				
Source(s)	**Meetings:** Daily FMPS and Testing Touch Base – September 3 & 9, 2013				
IVV Task: ST-2		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 2	**Verifiability:** Could not find evidence of test automation for the Sept. 6, 2013 delivery.	**3**	**4**	**12**	**Moderate**
Finding Detail	Could not locate specific documentation detailing use of test automation.				
Potential Impact	If the test automation artifacts are not available to the IV&V Team, then the Team cannot provide visibility into the quality or completeness of test automation.				
Recommendation	Document and make automation testing evidence available in CALT.				
Source(s)	**CALT:** doc53616 ACA FFM 09.06 PM Release Test Plan				

IVV Task: ST-2		Prob (P)	Impact (I)	Risk Score (P x I)	Risk Level
Finding 3	**Process Deviation:** Code implemented into production without being tested.	**5**	**3**	**15**	**High**
Finding Detail	It was stated at the "FMPS (Prod-Dev-Testing) Meeting" that code for Cost Sharing Reduction (CSR) was implemented into production without testing. It was also stated that in some instances, testing is only getting a half hour of time to test before code is implemented into production. This is possible because there are no testing or coding controls in place. The Test Manager stated, "The system will not pass financial audits. "				
Potential Impact	If code is implemented into production without being tested, then it may be deployed with defects.				
Recommendation	Develop a schedule and provide adequate time for testing prior to deployment to production. Reinstate the use of the testing playbook and appropriately update the playbook to provide clear direction regarding code base, test data and environments.				
Source(s)	**Meeting:** FMPS (Prod-Dev-Testing) Meeting – September 12, 2013				
IVV Task: ST-3	**Verify that an appropriate level of test coverage is achieved by the test process, that test results are verified, that the correct code configuration has been tested, and that the tests are appropriately documented, including formal logging of errors found in testing.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Process Deviation:** Test Readiness Reviews (TRR) are not being enforced consistently.	**5**	**2**	**10**	**Moderate**
Finding Detail	There was a lack of coordination among stakeholders regarding what was to be tested in each environment. There were problems with environmental readiness and test data. These were evidenced by the many issues being encountered in every environment and discussed at the 8:30 daily testing meeting. There were no best practice checks to ensure the code drops, the environment, and the data were ready before testing starts. It was also evidenced by the fact that main stakeholders like release management, Project Management Office (PMO), test teams were not made aware of the code being promoted.				
Potential Impact	If test environments are not ready, code drops are not understood, and test data is inadequate, then there is a risk that the code being tested is not the correct code, test environments may create issues, and time can be wasted.				
Recommendation	Hold regular TRRs. Verify that the test environments are ready, and populated with the correct test data to be in line with the code that is being tested. Inform the stakeholders exactly with what code is being tested, and supply the release notes prior to testing.				
Source(s)	**Meetings:** Daily FMPS and Testing Touch Bases Call – September 3, 2013 FMPS (Prod-Dev-Testing) Meeting – September 11, 2013				
IVV Task: ST-3		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**

Finding 2	**Completeness:** No test plans for Eligibility & Enrollment (E&E) and Plan Management (PM) from the CGI technical contractor.	**4**	**4**	**16**	**High**
Finding Detail	For the September 6, 2013 release version 6.4.0 for PM and the September 16, 2013 release version 7.0 for E&E deliveries, no evidence was found of test plans in CALT from CGI.				
Potential Impact	If test plans do not exist, then there may be inconsistency to testing and the approach may be unsystematic. The verification may be inadequate.				
Recommendation	CGI to make a test plan available for review in CALT.				
Source(s)	**CALT:** No Documentation Found				
IVV Task: ST-3		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 3	**Verifiability:** No evidence found in CALT for Affordable Care Act (ACA) testing of the September 16, 2013 delivery from the QSSI testing contractor.	**4**	**4**	**16**	**High**
Finding Detail	For the Eligibility & Enrollment (E&E) September 16, 2013 delivery, no evidence was found of testing in CALT from the QSSI testing contractor.				
Potential Impact	If test results are not available, then stakeholders may not be able to determine the risk is to the deployment of the product.				
Recommendation	QSSI should make test plans and results available in CALT.				
Source(s)	**CALT:** No Documentation Found				
IVV Task: ST-3		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 4	**Positive Finding:** Evidence was found in CALT that test summary reports document the code configuration that was tested for the September 6 and 16, 2013 deliveries.	**N/A**			
Finding Detail	There is evidence in CALT (doc50441 and doc51975) that identified the code configuration was documented for tests conducted on September 6 and 16, 2013 deliveries for the CGI Contractor.				
Potential Impact	N/A				
Recommendation	N/A				
Source(s)	**CALT:** doc50441 EE_R7.0_TestSummaryReport_Draft doc51975 EE_R7.0.1_TestSummaryReport				

IVV Task: ST-3		Prob (P)	Impact (I)	Risk Score (P x I)	Risk Level
Finding 5	**Testability:** Only 35% of the test cases executed passed for the release 7, September 16, 2013 delivery.	**4**	**4**	**16**	**High**
Finding Detail	Review of CALT doc51883 indicates the following: There was a total of 7,711 test cases with the follow statistics – • Blocked – 7.28% (561) • Failed – 39.84% (3072) • N/A - .84% (65) • No Run – 15.03% (1159) • Not Completed – 1.67% (129) • Passed – 35.34% (2725)				
Potential Impact	If adequate testing is not completed, then there is a risk that critical functions of the release will not be tested and unknown defects could be implemented.				
Recommendation	Run all planned test cases. Agree upon test results acceptance criteria. Ensure that testing results meets acceptance criteria before promoting the code.				
Source(s)	**CALT:** doc51883 EE_R7.0.1_TestCases				
IVV Task: ST-10	**Evaluate interface testing plans and procedures for compliance with industry standards.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Verifiability:** No evidence found in CALT for the September 6 and 16, 2013 deliveries that interface testing were conducted with the trusted partners.	**5**	**3**	**15**	**High**
Finding Detail	For the September 6 and 9, 2013 deliveries no evidence was found in CALT that integration testing with the trusted partners was executed; however, readiness testing activities were discussed at the “Daily Morning Production Call”.				
Potential Impact	If no evidence of integration testing is found in CALT, then the IV&V Team will not be able to provide visibility into the quality of the testing to upper management.				
Recommendation	Provide the appropriate documentation in CALT to prove that integration testing was conducted and shows successful results.				
Source(s)	**Meetings:** Daily Morning Production Call – September 3 and 17, 2013.				

IVV Task: ST-11	**Acceptance procedures and acceptance criteria for each product must be defined, reviewed, and approved prior to test and the results of the test must be documented. Acceptance procedures must also address the process by which any software product that does not pass acceptance testing will be corrected.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Completeness:** Inconsistent test data, test availability and coordination impacting UAT test execution.	**5**	**3**	**15**	**High**
Finding Detail	UAT testing has been delayed several times. It was stated that the test data provided doesn't match with the code drop and coordination of environment, data, time and other needed tasks to make it a successful test.				
Potential Impact	If code drops, test data, test environment availability and timing are not appropriately coordinated then there is a risk that UAT will not be executed and proven to be successful.				
Recommendation	Develop a schedule and provide adequate information regarding code to be tested, the environment that will be used for testing and the timing to appropriately coordinate the UAT.				
Source(s)	**Meetings:** Daily FMPS and Testing Touch Bases Call – September 3 and 17, 2013				
IVV Task: ST-11		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 2	**Process Deviation:** No acceptance testing documentation found in CALT.	**3**	**4**	**12**	**Moderate**
Finding Detail	Acceptance testing documentation was not found in CALT. No acceptance testing documentation was provided upon a document request. No evidence found in CALT of gate reviews held prior to acceptance testing.				
Potential Impact	If the government does not have an objective, independent review of acceptance testing, then the government will not be able to take corrective action over the unknown numbers of incomplete, incorrect, inconsistent, inaccurate test procedures, and acceptance criteria.				
Recommendation	Prepare acceptance criteria at the beginning of each sprint. Review acceptance criteria at the end of each sprint. Document acceptance criteria in CALT				
Source(s)	**CALT:** No Documentation Found				
IVV Task: ST-12	**Verify that appropriate acceptance testing based on the defined acceptance criteria is performed satisfactorily before acceptance of software products.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Verifiability:** No evidence was found of UAT plan or results	**5**	**2**	**10**	**Moderate**
Finding Detail	For the September 6 and 16, 2013 deliveries no evidence of UAT plans or results from CCIIO were found in CALT. However, daily project meetings indicated that UAT was being performed by CCIIO for the September 6 and 16, 2013 deliveries.				
Potential Impact	If UAT plans and results are not found in CALT then the appropriate level of testing may not be able to be verified for the deliveries including traceability to the functions being developed.				

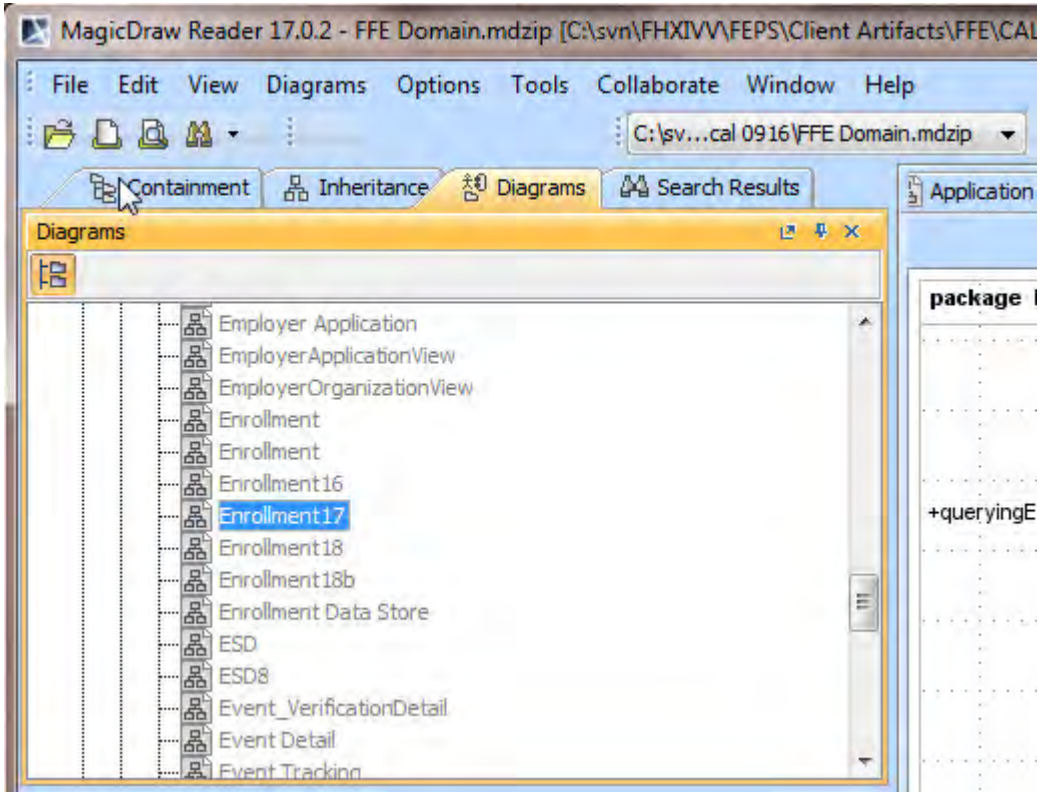
Recommendation	Provide UAT plans and results in CALT for review.				
Source(s)	**CALT:** No Documentation Found				
IVV Task: ST-15	**Review and evaluate implementation plan.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Inconsistency:** No evidence of a complete/comprehensive implementation plan found for FFM and FDSH.	**5**	**2**	**10**	**Moderate**
Finding Detail	For the FFM and FDSH release deliveries for September 6 and 16, 2013 no evidence was found in CALT of a complete/comprehensive implementation plan.				
Potential Impact	Without a comprehensive implementation plan that included schedule of activity including order and dependencies then critical task will be performed in the wrong order and task can be missed. • No data preparation requirements are specified • Timely submission of build notes • Missing performance monitoring procedures and implementation success criteria are specified • Implementation resources, contacts and roles are not identified				
Recommendation	Develop a complete and comprehensive implementation plan for the September 6 and 16, 2013 deliveries and store in CALT.				
Source(s)	**CALT:** No Documentation Found				
IVV Task: ST-15		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 2	**Testability:** No evidence found in CALT of performance testing for Release7 FFM.	**3**	**4**	**12**	**Moderate**
Finding Detail	No evidence of Performance monitoring procedures and execution of performance testing found for FFM release7 functionality.				
Potential Impact	If no performance testing is executed, then expected performance of the FFM application functions may not be known and be adequate to support the volume of applications causing a bad user experience.				
Recommendation	Plan for and provide evidence of performance testing execution for FFM.				
Source(s)	**CALT:** No Documentation Found				

2.7 FFM DATA MANAGEMENT FINDINGS

Table 2-7 FFM Data Management Findings

IVV Task: DM-1	Evaluate CMS's existing and proposed plans, procedures and software for data conversion.	Prob (P)	Impact (I)	Risk Score (P x I)	Risk Level
Finding 1	**Verifiability:** A Data Conversion Plan does not exist for the Federal Facilitated Marketplace.	**4**	**4**	**16**	**High**
Finding Detail	The FFM lacks a comprehensive Data Conversion Plan.				
Potential Impact	If a comprehensive Data Conversion Plan does not exist, then the program will lack transparency required to understand how data conversion processes are planned and executed which may produce significant downstream impacts affecting data quality, system performance, web services transactions, error rates and data transmission affecting all insurer data feeds and federal partner interfaces.				
Recommendation	Revisit the decision to waive the requirement for a Data Conversion Plan at least after initial product release. In Agile, it is common to use database refactoring to change informational semantics. You may need to write migration scripts. Database refactoring can be difficult in practice because of the coupling you're your source code, other application source code, data load source code, data extract source code, persistence frameworks and layers, your database schema, data migration scripts, test code, documentation and security impacts. A comprehensive data conversion approach should be developed based on DMBOK best practice recommendations. For example, it should minimally address the following: • Data conversion program requirements • Data quality procedures • Data validation procedures • Applicable Interface Control Document (ICD) source to target mapping • Data conversion formats • Data integration • Data stewardship • Data maintenance • Data clean up procedures • Error Rate Processes • Audit Procedures				

Source(s)	**CALT:** doc5205–FFE Process Agreements DRAFT V1.xlsx				
IVV Task: DM-5	**Evaluate new and existing database designs to determine if they meet existing and proposed system requirements.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Process Improvements:** It is not evident the Canonical Model Team, CGI and QSSI developers are communicating effectively.	**4**	**3**	**12**	**Moderate**
Finding Detail	IV&V emailed Noblis on August 14th, 2013 a series of questions to understand the following: • Who designed the Canonical Data Model for CMS? • Do you understand how CGI and FDSH developers used the Canonical Model to design the database and application? • How does CGI deploy code to MarkLogic database(s)? • Do you have any documents that can be shared with IV&V? Noblis responded to IV&V Aug 15th, 2013: • Our interactions with CGI and QSSI only go as far as the creation of exchange schemata. • We do not have interactions with the application developers, nor do we have any insight into how they develop any MarkLogic databases.				
Potential Impact	If ineffective communication between Noblis, CGI and QSSI continues, then application releases/updates may not satisfy requirements, and/or achieve traceability to the established Canonical Data Model. This may include: • Increased likelihood of additional defects having higher severity levels and complexity. • Poor application maintainability. • Hindered testing efforts and impacts to the customer experience in production.				
Recommendation	CMS should establish a RACI (Responsibility, Accountability, Consulted, and Informed) chart which addresses the unique roles and responsibilities for all the contractors involved in data management activities. CMS should increase its participation in the meetings between the parties and exercise leadership to ensure all requirements are satisfied in designs, configurations, and data management activities. CMS should establish quality completeness criteria checklists and ensure they are used at all major checkpoints and work product review discussions/approaches or strategies.				
Source(s)	**Email:** [redacted] **Meetings**: Wednesday Canonical meetings				
IVV Task: DM-5		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 2	**Consistency:** More than twenty Federally Facilitated Marketplace (FFM) Domain diagrams are inconsistently named and the names are not meaningful.	**3**	**3**	**9**	**Moderate**

Finding Detail	There are multiple diagrams that are not consistent. For example, diagrams: “Enrollment16”, “Enrollment17”, “Enrollment18”, “Enrollment18b”, “VerificationIncarceration”, “VerificationIncarceration11”, and “VerificationIncarceration13” are part of the “Eligibility and Enrollment” package. Based on how the diagrams were named, IV&V was unable to determine the diagram status i.e. (are they final or draft). IV&V found additional examples that were not named in this finding. The diagram below shows the inconsistent naming conventions. 
Potential Impact	If an established naming convention is not consistently followed then: • Diagram usability will increase in complexity. • Production/test environment debug efforts will be impeded.

Recommendation	The name of each diagram should be self-explanatory. IV&V recommends: • Contractors follow established naming conventions and consistently apply them. • Review all the diagrams in each package and update accordingly.				
Source(s)	**CALT:** FFE Domain.mdzip inside of doc51880 CMS E&E Delivery 09162013				
IVV Task: DM-6	**Recommend improvements to existing designs to improve data integrity and system performance.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Completeness**: There is limited informational content in most of the Multiple Canonical Model documents.	**4**	**4**	**16**	**High**
Finding Detail	The processes, plans and approaches captured don't comprehensively achieve the purpose and intent of the document. For example: • doc20820, doc22905, doc24055, and doc22935 don't follow CMS format guidelines. • doc24633 is incomplete. Only the introduction page is written, the remaining document is blank. • doc22903 Risk_Management_Plan.docx does not address Canonical Data Model risk management, risk mitigation, risk identification or the risk log. There is little to no informational details to provide a clear understanding in regard to how risks are being addressed.				
Potential Impact	If limited information is provided in key delivered documents, then common understanding of the plans, processes and checklists may produce unexpected results.				
Recommendation	Update the documents referenced in the finding to include: • Ensure the appropriate templates are used. • Establish document quality completeness checklists based on IEEE or similar quality best practices. • Establish a CMMI based quality document review process. • Develop Key Performance Indicator (KPI) metrics to evaluate document content quality and address gaps to ensure consistency.				
Source(s)	**CALT:** doc22905 WBS_with_Dictionary.docx doc24055 Communications_Plan.docx doc20820 Project_Scope_Statement.docx doc22935 CIEM_Checklist.docx doc24633 Change_Management_Plan.docx doc22903 Risk_Management_Plan.docx				
IVV Task: DM-8	**Evaluate the project's process for administering the database, including backup, recovery, performance analysis and control of data item creation.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Verifiability and Completeness:** There is no evidence that E&E & QHP address Disaster Recovery Procedures.	**4**	**4**	**16**	**High**

Finding Detail	Page 29, Section 5.3 Recovery Procedures, states "Disaster Recovery is not a requirement for QHP." The document fails to mention that E&E backup and recovery is needed. The lack of E&E and QHP disaster recovery procedures promotes "a hero" solution which is highly risky because it's both untested and not recommended by any external best practice or competing CMS internal guideline.				
Potential Impact	If the system experiences an outage resulting in the loss of files/data/use, then it could be chaotic if not impossible to recover and restore data causing a disruption of service in production for an in-determined period of time.				
Recommendation	Update the Recovery Procedures to include appropriate detailed steps to restore and recover EE and QHP data. Ensure the instructions are consistent with similar instructions that may exist in other documentation i.e. security plans, FFM high level technical documents etc… Ensure the recovery procedures satisfy service level agreements and other applicable business requirements.				
Source(s)	**CALT:** doc53081 EE_R7.0.1_OMM.docx				
IVV Task: DM-8		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 2	**Completeness:** Database recovery, backup procedures and performance analysis are incomplete.	**5**	**5**	**25**	**High**
Finding Detail	It's not evident these areas are adequately addressed based upon the documentation reviewed. For example the MarkLogic Configuration for Prod Prime Go Live (June 2013) document indicated: "TODO : Future version of this document or a separate document may cover the following Common Operational Procedures • Common Operational Procedures • Backup? • Recovery from Backup? • Running a CoRB • Reference Data Migration "				
Potential Impact	If backup and recovery procedures are incomplete, then program execution and delivery will be seriously affected.				
Recommendation	Update the documentation which reflects MarkLogic recommended guidance and address system and business requirements.				
Source(s)	**CALT:** MarkLogic Configuration for Prod Prime Go Live (June 2013) embedded in doc53030 FDF36-CMS-ACA-SPR-092313				
IVV Task: DM-8		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 3	**Completeness**: Local Database Backup Procedures are not comprehensively addressed in the E&E Operations Maintenance Manual (doc53081).	**4**	**4**	**16**	**High**

Finding Detail	In the EE_R7.0.1_OMM (doc53081), Local backup procedures don't provide sufficient details to understand the step by step tasks involved to satisfy local backup requirements. For example, backup procedures should address: roles/responsibilities, media to be used, scripts, permissions, specific data requirements, testing considerations, servers and other hardware implicated, etc… None of that detail was provided. Activities captured should include a workflow and a RACI. The specific performance requirements associated with the backup are also not addressed. Who will be notified should a backup be necessary? Timing considerations are not addressed; for example, how long is it expected for a backup to start and complete successfully? The System Design Document (doc51919) states that "Terremark supplies resource allocation, an online backup system, and a host intrusion detection system (IDS). URS provides all infrastructure support of the environments, including back-up operations, monitoring and maintaining the operating systems. CGI Federal provides operations, monitoring, and maintenance of the application/Commercial Off-The-Shelf (COTS) software and the FFM application… The backup and recovery approach is described in details in the Contingency Plan document." And Contingency Plan document cannot be located in CALT.				
Potential Impact	The lack of backup details may severely impact the ability of the program to satisfy restore requirements. The lack of backup details implies knowledge required to perform a local restore may reside in few resources and therefore presents a risk to the program should those resources be unavailable.				
Recommendation	Update the local database backup procedures with a set of comprehensive steps and activities. Ensure MarkLogic and Oracle database best practices are leveraged.				
Source(s)	**CALT:** doc53081 EE_R7.0.1_OMM doc51919 EE_R7.0.1_SystemDesignDocument				
IVV Task: DM-8		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 4	**Completeness**: Re-start procedures and E&E application monitoring are not comprehensively addressed in the Operations Maintenance Manual (doc53081).	**2**	**4**	**8**	**Moderate**
Finding Detail	As a best practice, each task and command should reflect the expected duration to successfully execute a command. In addition, any errors that may be encountered should be captured with an appropriate work around.				
Potential Impact	If no details are provided and/or if restart fails then the executer won't have appropriate instructions necessary to resolve the issue. The lack of details may severely impact the ability of the program to satisfy restart requirements.				
Recommendation	Update the restart procedures with a set of comprehensive steps and activities including trouble shooting. There should be a notification process with specific roles identified in executing the commands and a notification to parties/resources that are expected to remain informed during the restart procedure. These procedures should also be reflected as having been "tested" to develop benchmarks and ensure the procedures work.				
Source(s)	**CALT:** doc53081 EE_R7.0.1_OMM				

IVV Task: DM-8		Prob (P)	Impact (I)	Risk Score (P x I)	Risk Level
Finding 5	**Completeness:** MarkLogic Configuration for Prod Prime Go Live (June 2013) does not provide comprehensive setup information.	**2**	**4**	**8**	**Moderate**
Finding Detail	The configuration guide deviates from general format instructions in similar CMS documentation. The document is still in "draft", however, it should have been in a final "approved" status given the go-live occurred in June 2013. The guide overall is not adequately detailed to understand the entire process to setup MarkLogic for the Prod Prime environment. The document doesn't contain database design details.				
Potential Impact	If the documentation lacks adequate details in scope and content regarding database configuration, timing and installation instructions, then ACA processes may be delayed.				
Recommendation	CGI should update the document with appropriate details describing the steps and approach necessary to successfully setup MarkLogic in all environments (for example the development, testing, and production).				
Source(s)	**CALT:** MarkLogic Configuration for Prod Prime Go Live (June 2013) embedded in doc53030 FDF36-CMS-ACA-SPR-092313				
IVV Task: DM-8		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 6	**Correctness:** Inadequate retention of Audit Logs in MarkLogic.	**4**	**4**	**16**	**High**
Finding Detail	It is unclear 7 days retention of audit logs represents a CMS requirement for meeting auditability. For example, Page 14, Auditing states "Retention of Audit Logs in MarkLogic is currently 7 days."				
Potential Impact	If the current retention of audit logs does not provide CMS with sufficient history to perform root-cause analysis then the resolution of production issues may be impeded.				
Recommendation	The approach should be reviewed against current CMS retention of audit log requirements to ensure the best possible outcome is achieved to minimize risks and promote optimal issue resolution.				
Source(s)	**CALT:** MarkLogic Configuration for Prod Prime Go Live (June 2013) embedded in doc53030 FDF36-CMS-ACA-SPR-092313				
IVV Task: DM-8		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 7	**Completeness:** Approach to accomplish logical segregation by business area is not fully documented.	**3**	**4**	**12**	**Moderate**
Finding Detail	It's unclear if other approaches are being employed or considered to accomplish logical segregation by business area. For example, page 7 of the MarkLogic Configuration for Prod Prime document states: "Generally, in Prod Prime we will use Role Based Access Control (RBAC) to logically segregate data by business area. This means we will have the option of storing data from two different business areas within the same physical database and forests".				

Potential Impact	If the approach to accomplish logical segregation by business area is inconsistent then unknown results may significantly impact performance.				
Recommendation	Specify all approaches that are or will be used to accomplish logical segregation by business area to ensure diverse data is stored into the appropriate physical database and forests. Documenting all approaches provides necessary transparency and supports performance requirements.				
Source(s)	**CALT:** MarkLogic Configuration for Prod Prime Go Live (June 2013) embedded in doc53030 FDF36-CMS-ACA-SPR-092313				
IVV Task: DM-8		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 8	**Correctness:** The approach for managing database passwords lacks critical details.	**5**	**5**	**25**	**High**
Finding Detail	The preferred approach for managing database passwords may introduce additional risks and therefore presents unacceptable risks for compliance with CMS password policy. The approach lacks the following details: • Who will monitor the password? • Who will be the Point of Contact for each project? • What is the contact information of each contact i.e. (name, phone number, email)? • How many projects are affected? • How many property files are being used to connect to the database? • Identify the name/location/path/server name of the property files etc… • What are the logical steps/procedures to execute manage data base passwords? E.g. (bring down Jboss, change property file password, change database (DB) password, change MIDAS data extract file connection to MarkLogic DB etc.				
Potential Impact	If detail procedures are not included, then CMS compliance with 60 day password policy may not be achieved.				
Recommendation	The approach should reflect the finding details above.				
Source(s)	**CALT:** MarkLogic Configuration for Prod Prime Go Live (June 2013) eembedded in doc53030 FDF36-CMS-ACA-SPR-092313				
IVV Task: DM-8		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 9	**Correctness:** Roles and permissions assigned in configuration guide are not consistent with the MarkLogic XML Counterbase Connector (XCC) Developer's Guide.	**3**	**3**	**9**	**Moderate**

Finding Detail	The approach described for managing roles and permission does not appear to be consistent with section XCC Developer's Guide 2.9.2 Predefined Security Roles for Extended Architecture (XA) Participation. As stated in the XCC Developer's Guide: • The XA user role allows creation and management of one's own XA transaction branches in MarkLogic Server. • The XA-admin role allows creation and management of any user's XA transaction branches in MarkLogic Server. • The XA role is required to participate in XA transactions. The XA-admin role is intended primarily for Administrators who need to complete or forget XA transactions However, the roles and permissions in the MarkLogic Configuration for Prod Prime document assigns "XA" and "XA-admin" permissions to all read-only roles for many projects. The table contains a sample of evidence supporting the finding:

Role	Inherits Roles	Inherits built-in roles	Exec Privileges/Default Document Permissions
FMPS-modules		XA, XA-admin	
indvmatch-readonly	FMPS-module		Execute Priv: http://cms.hhs.gov/FMPS/indvmatch/execute
indvmatch-dal	indvmatch-readonly FMPS-writer		Doc permission: indvmatch-readonly – read Doc permission: indvmatch –dal – insert Doc permission: indvmatch –dal – update Doc permission: indvmatch –dal – execute
ffe-readonly	FMPS-modules		Execute Priv: http://cms.hhs.gov/FMPS/ffe/execute
fed-readonly	FMPS-modules		Execute Priv: http://cms.hhs.gov/FMPS/fed/execute
fed-dal	fed-readonly FMPS-writer		Doc permission: fed-readonly – read Doc permission: fed-dal – insert Doc permission: fed-dal – update Doc permission: fed-dal – execute

Potential Impact	If consistency roles and permissions are not consistently and comprehensively addressed, then maintainability issues may affect database performance and web services transactions.
Recommendation	The approach should be consistent with MarkLogic best practices outlined in The XCC Developer's Guide. Minimally, read-only roles should not have privileges for creation and management of any user's XA transaction branches. CGI/CMS should re-evaluate the process. Perhaps only the XA role is needed but not the XA-admin.

Source(s)	**CALT:** MarkLogic Configuration for Prod Prime Go Live (June 2013) embedded in doc53030 FDF36-CMS-ACA-SPR-092313 **Website:** http://docs.marklogic.com/guide/xcc.pdf – Marklogic Sever XCC Developer's Guide

2.8 FFM OPERATIONS OVERSIGHT FINDINGS

Table 2-8 FFM Operations Oversight Findings

IVV Task: OO-5	Evaluate operational plans and processes.	Prob (P)	Impact (I)	Risk Score (P x I)	Risk Level
Finding 1	**Correctness:** The ACA System Security Plan (SSP) template is not being used for SSPs.	**2**	**2**	**4**	**Low**
Finding Detail	The SSP template used is dated 2009. CMS has a special ACA SSP template dated 2012 that included all of the information needed to be compliant with Internal Revenue Service (IRS) SSP requirements.				
Potential Impact	If the incorrect template is not used, then some information may be missing. If this template should not be used, then it should be removed from the CMS website.				
Recommendation	Update the SSPs or remove the template from the CMS website.				
Source(s)	**CALT:** doc53567 Final SSP DSH **CMS Website:** ACA-SSP-Template-v-1-0-012012-a				
IVV Task: OO-5		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 2	**Correctness:** Authorization appears to have been granted for FFM operations while there are 2 high findings from the SCA.	**5**	**5**	**25**	**High**
Finding Detail	The Final Platform as a Service (PaaS) Findings from QHP CMS FISMA Control Tracking System (CFACTS) Spreadsheet – PDF states that there are two High findings from the SCA that were not closed: • "Macros enable on uploaded files allow code to execute automatically" (High Likelihood, High Impact). • "No evidence of functional testing processes and procedures being adequate to identify functional problems resulting in nonfunctional [sic]code being deployed" (High Likelihood, High Impact). From the Health Insurance Oversight System (HIOS) Findings from QHP CFACTS Spreadsheet – PDF states there is one High finding from the SCA: • "The Login and establishment of session cookies is not fully secured using HTTPS. Sessions cookies exposed under http are unencrypted and can be see [sic] in the clear, which may facilitate in session Hijacking." (High, High)				
Potential Impact	• (Issue) CMS accepted the risk and consequences of nonfunctioning code. • If the "enabled" macros enable the insertion of a computer virus into the marketplace, then a security incident may occur.				

Recommendation	• Follow the security Guide established by the Office of the Chief Information Security Officer (OCISO).				
Source(s)	**CALT:** doc29074 PaaS Findings from QHP CFACTS Spreadsheet - PDF doc29071 HIOS Findings from QHP CFACTS Spreadsheet - PDF **CMS Security Website:** OCISO CMS Information Security (IS) Authorization To Operate Package Guide, FINAL Version 3.0, December 1, 2011.				
IVV Task: OO-6	**Evaluate implementation of the process activities including backup, disaster recovery and day-to-day operations to verify the processes are being followed.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Completeness:** There is no Disaster Recovery (DR) site for FFM.	**3**	**5**	**15**	**High**
Finding Detail	• No DR status was provided during the pre and post-Deployment meetings even though they were part of the checklists. • No apparent CALT documentation provides the status of the HP DR site, which was supposed to be ready by Oct. 1. • The signed Certification Letter (doc45165) does not name the absence of the DR site as a weakness of note. • The current FFM IS Contingency Plan (ISCP) (in CALT) states, "The implementation of the Disaster Recovery (DR) warm site located in Terremark's NAP of the Americas facility in Miami, FL has been postponed. It is planned that the primary and DR sites will transfer to Hewlett-Packard (HP) under the Virtual Data Center (VDC) contract in calendar year 2014." • The FFM ISCP states that the Recovery Point Objective (RPO) and Recover Time Objective (RTO) are 24 hours. • Doc53081 does not address database Capacity planning. IV&V presented the following question to Terremark on May 23rd, 2013 during an interview: "Why does the Disaster Recovery Failover site not provide enough space to support failover and recovery", Terremark's response was "…the decision was made by the project owner." • It's not evident that Disaster Recovery can be verified due to contradictions in the documentation: For example, doc51919 chapter 9 – Backup and Recovery Approach states "The warm DR site supports a RTO of 24 hours and a RPO of 24 hours." However based on CCIIO Resource Allocations by Project – ECPE Cloud 20130517.pdf, the Disaster Recovery site for FFM has not been setup yet. Row 7 " FFE Project Total" of the figure below, there are no Virtual Machine (VM) servers setup at the DR site.				

CCIIO Cloud Resource Allocations by Project (as provisioned)

	Culpeper				Miami (DR Failover)			
	Virtual Machines (VMs)	Processors (#VPUs)	Memory (GB)	Storage (GB)	Virtual Machines (VMs)	Processors (#VPUs)	Memory (GB)	Storage (GB)
CALT Project Total	37	74	240	7050	6	10	18	794
CMMI Project Total	9	36	144	2240	0	0	0	0
CMSNet Project Total	3	4	28	275	0	0	0	0
DSH Project Total	171	684	2126	33320	0	0	0	0
ECWS Project Total	66	146	449	10529	0	0	0	0
EIDM Project Total	67	310	700	13540	0	0	0	0
FFE Project Total	237	607	2950	103563	0	0	0	0
HIAD Project Total	3	6	30	260	0	0	0	0

Potential Impact	If a disaster occurs during this time of no coverage:
	• The Federally-Facilitated Marketplace systems will not be able to operate until
	  ○ An agreement is executed with Verizon or HP.
	  ○ Components are procured, set up and backups are restored.
	• CMS will gain further bad press.

Recommendation	• Establish a DR site as soon as possible. • Document a contingency plan for recovery during the period that there is no DR site. • Establish National Institute of Standards and Technology (NIST) controls as a standard. • Processes and procedures must address synchronization of primary site data files with failover site data files to ensure the failover site becomes the new primary when/if the primary site is lost. • The DR Failover site should be a hot backup site.
Source(s)	**Email:** CMS Marketplace Checklist – 9-24-13_v10, p. 59; Pre-Deployment ORR PRR_Meeting Capture_09212013, p. 7. **CALT:** doc45165 FFM CA Memo_08-08-2013.pdf doc53729 HIX-A Draft SCA Report for Aug & Sept 2013 MITRE-led SCAs with CGI's Comments doc50837 FFM Contingency Plan September 2013 doc53081 EE_R7.0.1_OMM.docx; doc51919 EE_R7.0.1_SystemDesignDocument.docx **GTL:** CCIIO Resource Allocations by Project – ECPE Cloud 20130517.pdf

3 FDSH

An in-depth review of the code was performed for FDSH, as well as assessments of the documentation received after November 15, 2012. The findings from these assessments are categorized in accordance with the IV&V Scope of Services laid out in the FMPS IV&V Statement of Work (SOW).

3.1 FDSH QUALITY MANAGEMENT FINDINGS

Table 3-1 FDSH Quality Management Findings

IVV Task: QA-3	**Verify that the QA organization monitors the fidelity of all defined processes in all phases of the project.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Positive Finding**: Monitoring the fidelity of defined processes is consistent.	**N/A**			
Finding Detail	QSSI conducts CMMI-based process evaluations on a regular basis.				
Potential Impact	N/A				
Recommendation	N/A				
Source(s)	**QSSI:** Process Health Review (PHR) workbook.				
IVV Task: QA-4	**Verify that the quality of all products produced by the project is monitored by formal reviews and sign-offs.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Consistency:** The sign-off process is inconsistent.	**4**	**2**	**8**	**Moderate**
Finding Detail	Sign-off of documents in CALT is not consistent some documents do not have sign off/ approval pages. When approval pages are present sign off is not done.				
Potential Impact	If approval is not made then development of unapproved processes may occur impacting customer use and performance				
Recommendation	Ensure that all documentation that requires approval have signatures verified upon delivery.				
Source(s)	**CALT:** doc27080 FDSH_DEV_PROC				
IVV Task: QA-5	**Verify that project self-evaluations are performed and that measures are continually taken to improve the process.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Positive Finding:** Evaluation and update of internal processes are performed.	**N/A**			

Finding Detail	After each delivery and at lesson learned meeting the internal processes are reviewed and updated as appropriate.				
Potential Impact	N/A				
Recommendation	N/A				
Source(s)	**QSSI:** Process Health Review (PHR) workbook.				
IVV Task: QA-10	**Review and make recommendations on all defined processes and product standards associated with the system development.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Positive Finding:** QSSI follows traditional QA product and process standards, including Agile development	**N/A**			
Finding Detail	FDSH_DEV_PROC (doc27080) contains the procedures and standards used including Agile development				
Potential Impact	N/A				
Recommendation	N/A				
Source(s)	**CALT:** doc27080 FDSH_DEV_PROC				
IVV Task: QA-11	**Verify that all major development processes are defined and that the defined and approved processes and standards are followed in development.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Positive Finding:** The QSSI development group follows detailed and defined processes.	**N/A**			
Finding Detail	Processes and procedures for the development group are defined and followed as evidenced by QA Audits.				
Potential Impact	N/A				
Recommendation	N/A				
Source(s)	**QSSI:** Process Health Review (PHR) workbook.				
IVV Task: QA-13	**Verify that all process definitions and standards are complete, clear, up-to-date, consistent in format, and easily available to project personnel.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Positive Finding:** Internal processes and procedures follow a standard format and are available to all users	**N/A**			
Finding Detail	Internal processes and procedures follow a standard format and are available to all users working in the development group.				
Potential Impact	N/A				
Recommendation	N/A				
Source(s)	**QSSI:** Process Health Review (PHR) workbook.				

3.2 FDSH TRAINING FINDINGS

Table 3-2 FDSH Training Findings

IVV Task: TR-1	**Review and make recommendations on the training provided to system users. Verify sufficient knowledge transfer for maintenance and operation of the new system.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Positive Finding:** FDSH_IMP_OMM provide sufficient knowledge transfer for maintenance and operation of the new system.	**N/A**			
Finding Detail	The FDSH_IMP_OMM provides sufficient knowledge transfer for maintenance and operation or the new system by extensively covering the following areas: • System (Functional; Application/System Dependency; Physical; System User; Processing; Security and Privacy) • Operational and Maintenance Responsibility • Operations Procedures (Operations Sequence; Procedures; Backup; Restart/Recovery; Monitoring; Maintenance) • Data and Database Administration • Configuration Management (Configuration Identification; Configuration Control; Release Management; Configuration Integrity)				
Potential Impact	N/A				
Recommendation	N/A				
Source(s)	**CALT:** doc26320 FDSH_IMP_OMM				
IVV Task: TR-1		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 2	**Completeness:** No evidence found of comprehensive training for integration testing with the trusted partners.	**4**	**2**	**8**	**Moderate**
Finding Detail	There was no evidence found in CALT to indicate that training transpired in preparation for integration testing with the trusted partners however Secure Communications – Application Later Connectivity Test for SSA, IRS, DHS documentation provide detail interface test cases that provide guidance on testing.				
Potential Impact	If training does not happen then there is a risk that integration testing users may not be adequate prepared when executing integration testing.				
Recommendation	Provide plans and training for integration testing with the trusted partners and publish in CALT.				

Source(s)	**CALT:** doc29501 Secure Communications – Application Later Connectivity Test (SSA) doc45582 Secure Communications – Application Layer Connectivity Test (IRS) doc29440 Secure Communications – Application Layer Connectivity Test (Medicare)				
IVV Task: TR-4	**Verify that all necessary policy and process and documentation is easily available to users.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Positive Finding:** CM plan provides policies and procedures to the user.	**N/A**			
Finding Detail	The FDSH Configuration Management Plan can provide the user (in this case the developer) with the necessary policies and processes for developing the system found in the following sections: 3.2 – System Architecture 5.1 – Methods and Tools 5.4 – Environment 6.1 – Configuration Identification 6.2 – Configuration Control				
Potential Impact	N/A				
Recommendation	N/A				
Source(s)	**CALT:** doc53568 FDSH_Plan_Configuration_Management				
IVV Task: TR-4		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 2	**Completeness**: Proprietary Link provided in CM plan for additional information regarding Change Management.	**5**	**1**	**5**	**Low**
Finding Detail	Section 6.2.1 “Change Management” contains a link to the QSSIQ site for more detail on the project change management process and requires sign on credentials to access the site.				
Potential Impact	If a user needs access to more details regarding change management and does not have the sign on credentials then the user will not be able to access the change management information.				
Recommendation	Provide the additional details regarding change management within the FDSH_Plan_Configuration_Management and do not require the user to sign on to another repository for the information.				
Source(s)	**CALT:** doc53568 FDSH_Plan_Configuration_Management				
IVV Task: TR-4		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**

Finding 3	**Completeness:** No evidence found of formal training for users (IRS, SSA, Peace Corps) of the FDSH.	**5**	**1**	**5**	**Low**
Finding Detail	No evidence found that formal training occurred for IRS, SSA and Peace Corps users of the FDSH. BSDs will describe and provide guidance on how to use the use the interfaces to the FDSH.				
Potential Impact	If formal training is not provided then there is a risk that use of the FDSH interfaces may not be interpreted correctly causing confusion and wasted time.				
Recommendation	Provide and store training documentation in CALT				
Source(s)	**CALT:** No Documentation Found				

3.3 FDSH REQUIREMENTS MANAGEMENT FINDINGS

Table 3-3 FDSH Requirements Management Findings

IVV Task: RM-6	Evaluate and make recommendations on project policies and procedures for ensuring that the system is secure and that the privacy of client data is maintained.	Prob (P)	Impact (I)	Risk Score (P x I)	Risk Level
Finding 1	**Process Improvement:** Follow good software engineering practices.	**5**	**2**	**10**	**Moderate**
Finding Detail	The HP Fortify test results show a significant number of coding issues that could have been avoided. These include: "As of 7/15/2013, HP Fortify discovered a total of 484 issues including 17 OWASP [Open Web Application Security Project]-related security issues, 50 FISMA-related violations and 8 2010 CWE [Common Weakness Enumeration]/SANS Top 25 security findings, which results in a technical risk rating of Medium and failure of the FIPS-200 portion of FISMA compliance." This supports Assessment#3, TR-6, Finding #1, "**Completeness**: There is no evidence of secure coding training being provided to developers." Still applies. This is still an open finding.				
Potential Impact	If the development team does not follow secure coding practices, then there will be a significant effort in fixing the code afterward. This could result in higher project costs and schedule slippages.				
Recommendation	• Ensure secure coding practices are implemented during development.				
Source(s)	**CALT:** doc43593				
IVV Task: RM-7	**Evaluate the projects restrictions on system and data access.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Completeness:** There are 15 (14 moderate and 1 low risk) findings remaining from the independently-performed Security Controls Assessment of FDSH that amount to higher degree of risk as a whole.	**4**	**4**	**16**	**High**

Finding Detail	These findings include: • No review of rogue Partner IDs (Moderate). • All IP traffic is allowed by firewall between data and application zones (Moderate). • System Security Plan is incomplete (Moderate). • Servers running databases in the Application Zone (Moderate). • Incomplete Contingency Plan (Moderate) – this is documented as a separate IV&V finding because of the extent to which the plan is incomplete. • Incomplete Risk Assessment (Moderate) – this is documented as a separate IV&V finding because of the extent to which the RA is incomplete. • The CFACTS SSP is incomplete (Moderate). • Database account passwords expire after 180 days instead of 60 (Moderate). • Database password reuse time in unlimited and reuse max is 720 (Moderate). • Database account lock is set as low as 1 day instead of unlimited (Moderate). • NonDBA users have system privileges (Moderate). • "Any" schema privileges given to nonDBA accounts (Moderate). • Audit logs only maintained for 7 days instead of 1 year requirement (Moderate). • ISAs/MOUs not in place at time of "go live" (Moderate). • Business risks not documented in ISRA (Low). All of this is a significant amount of risk to be accepting at the time of the ATO, and the highlighted areas represent areas where project restrictions on system and data access do not meet minimum federal control standards.				
Potential Impact	If there are a significant number of open, moderate risks at the time the system goes into Production, then the overall risk to confidentiality, integrity and availability may be high.				
Recommendation	Close these areas as soon as possible.				
Source(s)	**CALT:** doc54780 DSH SCA CFACTS Spreadsheet				
IVV Task: RM-8	**Evaluate the projects security and risk analysis.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Verifiability and Completeness:** The FDSH IS Risk Assessment in CALT is not complete.	**5**	**3**	**15**	**HIGH**

Finding Detail	The missing components to the IS RA are: • IS RA Date: • IS RA Version Number: • Risks and Safeguards – there are none This is basically the same status as when the IS RA Evaluation was performed by MITRE (doc47375). The IV&V team does not have access to CFACTS to determine whether or not the RA was updated.				
Potential Impact	If the FDSH IS RA is not complete, then it cannot be verified by IV&V for residual security risk.				
Recommendation	Complete the FDSH IS Risk Assessment and post it in CALT.				
Source(s)	**CALT:** doc14169 HIX DSH IS Risk Assessment doc47375 DSH RS Evaluation				
IVV Task: RM-9	**Verify that processes and equipment are in place to back up client and project data and files and archive them safely at appropriate intervals.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Verifiability:** Duplicate documents in CALT may confuse the user as to processes & procedures (doc12881 and doc7475).	**5**	**1**	**5**	**Low**
Finding Detail	Documents doc12881 “Backup and Restore Services procedures” dated October 9, 2012 and doc7475 “Ecloud Backup Process Document 05_08_2012” dated May 17, 2012 contain identical information but have different file names in CALT.				
Potential Impact	If duplicate documents exist in CALT then, confusion and schedule impacts may occur if updates are made to one of the documents and the other document is referenced by the user.				
Recommendation	Determine which document should be retained in CALT and delete the duplicate document.				
Source(s)	**CALT:** doc12881 Backup and Restore Services procedures doc7475 Ecloud Backup Process Document 05_08_2012 doc12885 OM Manual eCAP				
IVV Task: RM-9		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 2	**Correctness and Completeness:** The FDSH IS Contingency Plan (ISCP) has content errors and is incomplete.	**3**	**4**	**12**	**Moderate**

Finding Detail	The FDSH ISCP has the following correctness issues: • Terremark is providing DR services. • There is no integration with the XOC Crisis Management Bridge Protocol or SOP. • The ISCP states "a Recovery Time Objective (RTO) of 24 hours and a Recovery Point Objective (RPO) of 24 hours." Whereas, the SCA Report points out the contradiction in the RTO of 4 hours. The SCA Report states, "During the contingency planning interview it was noted that the system was not a mission critical system, but per the SSP, the ISSO interview and the contingency planning interview, the current stated requirement for availability was 24 hours with the expectations that **the FDSH be available within 4 hours of failure** in the future." This is a contradiction that needs to be resolved. • Also, the Hub is designated as not mission critical. Since it is mandated by law, this seems incorrect. The FDSH ISCP completeness issues are: • There are 19 TBDs in the plan. • The Recovery Team contact list does not include contact information for the XOC. • The Recovery Team contact list does not include contact information for Terremark. • A contact list footnote states that the ISCP is being revised to be integrated with the XOC. • The ISCP is designated "Draft" in CALT. • The evaluation checklist provided by MITRE shows that 70% of the items are partially met and 4% are not met.				
Potential Impact	If the ISCP is incomplete at the time an event occurs that impacts FDSH, then the ISCP may be inadequate for use in recovering from the event.				
Recommendation	Update the IS CP as soon as possible.				
Source(s)	**CALT:** doc48809 DSH CP Document - 08/29/2013 doc53047 DSH - DRAFT SCA REPORT Sept 2013				
IVV Task: RM-9		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 3	**Completeness:** The Contingency Plan (CP) Test tabletop exercise was inadequate.	**4**	**4**	**16**	**HIGH**

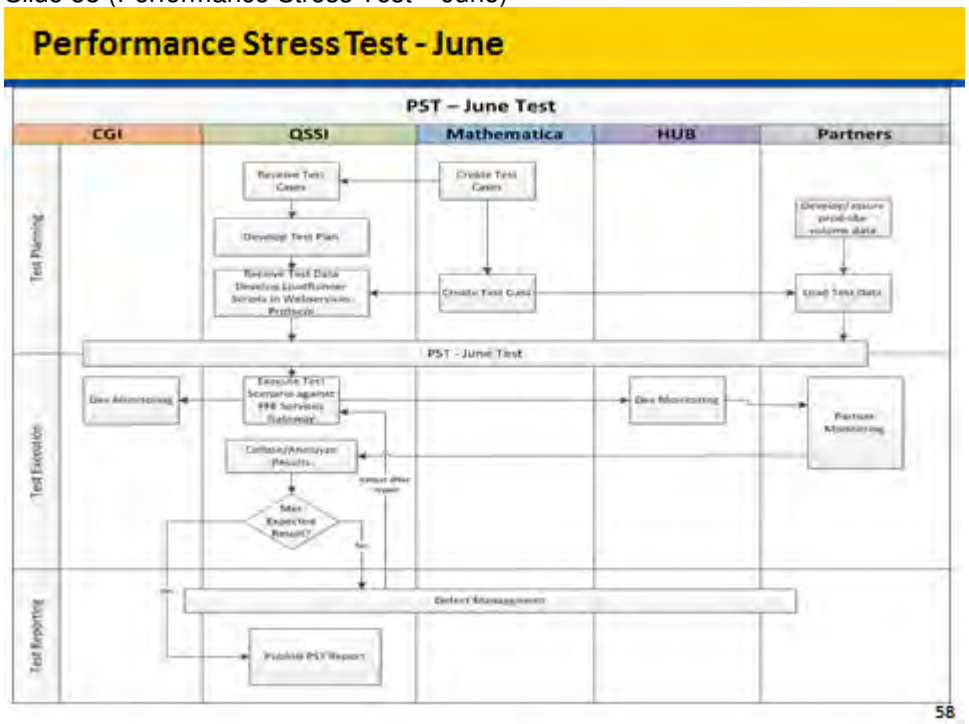
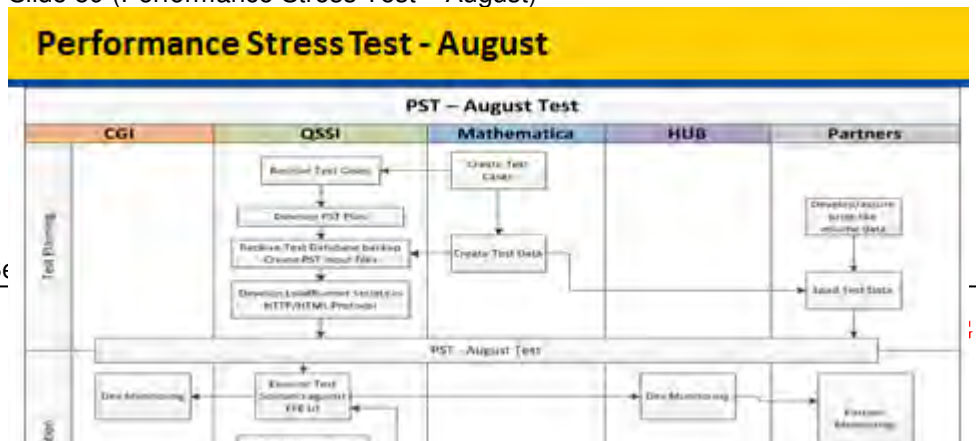
Finding Detail	• There was only one scenario reflective of a hardware abnormality. • There was no evidence that the XOC Crisis Management Bridge Protocol and SOP were included in the test. However, one person from the XOC team did participate in the exercise, but it is not clear what steps he performed. • No one was present to represent the business and end users. • Only a Type A, lowest priority tabletop test, was conducted. • The FDSH SSP states, “The process will be coordinated with the XOC and Terremark to verify roles and responsibilities are known.” • NIST CP-4 Supplemental Guidance states that the test should include other related plans. The XOC does have a Crisis Plan and the FDSH IS CP states that the XOC is involved in all contingency plan activities. • This one test scenario does not appear to be realistic and comprehensive. Although NIST states that the breadth and depth of the exercises are up to the responsible organization, IV&V believes this is inadequate.
Potential Impact	If a realistic exercise is not performed of the FDSH CP, then the organization may not be prepared for the reality of exercising the CP.
Recommendation	• Conduct a tabletop exercise that includes the XOC and business users. • Ensure the test includes scenario (s) that completely exercises the CP.
Source(s)	**CALT:** doc48809 DSH CP Document - 08/29/2013 doc46710 HUB-CP-Table Top Test_08162013_JK Corrected.docx doc53567 Final SSP DSH **Standard:** NIST 800-53 r4

3.4 FDSH OPERATING ENVIRONMENT FINDINGS

Table 3-4 FDSH Operating Environment Findings

IVV Task: OE-1	Evaluate new and existing system hardware configurations to determine if their performance is adequate to meet existing and proposed system requirements.	Prob (P)	Impact (I)	Risk Score (P x I)	Risk Level
Finding 1	**Verifiability:** Evidence of FDSH metrics on new and existing system hardware configurations performance is not present in CALT.	**5**	**5**	**25**	**High**
Finding Detail	doc41501 FDSH Release 6 – Performance Test Plan, pg. 7, Monitored Metrics "…Throughout all stages of testing, the Team collects the following metrics): • Application JMS Queue message sizes and growth statistics • Central Processing Unit (CPU) usage over time • Disk usage over time • Error ratios • JVM garbage collection timings and frequencies • JVM heap size over time • MarkLogic module invocation statistics • Minimum, maximum, and average response times • Network usage over time • RAM usage over time • Transactions per second				
Potential Impact	If no "Transaction Volume Estimates" exists, it will be difficult to determine and analyze whether the hardware performance is adequate in the production environment.				
Recommendation	Provide "Transaction Volume Estimates" spreadsheet – only available on QSSI portal. Verify performance monitoring software and parameters to ensure hardware performance is being adequately monitored to fulfill the business need.				
Source(s)	**CALT:** doc42643 FDSH_R6_Performance_Testing_Results, doc41501 FDSH Release 6 – Performance Test Plan, doc25400 FDSH_PLAN_PMPerformance_v1_0_D, doc41500 DSH_Plan_Transfer_Performance_Testing_Results Data Services Hub\Trackers > **List Trackers and Planning Folders**				

IVV Task: OE-8	Determine if the database's data format is easily convertible to other formats, if it supports the addition of new data items, if it is scalable, if it is easily refreshable and if it is compatible with the State's existing hardware and software, including any on-line transaction processing (OLTP) environment.	Prob (P)	Impact (I)	Risk Score (P x I)	Risk Level
Finding 1	**Verifiability –** No evidence available in CALT of test results regarding the importing and exporting features.	**3**	**2**	**6**	**Moderate**
Finding Detail	Data is the most, critical and key element in the solution. Test plans and test results for the import export feature are not available in CALT.				
Potential Impact	If proper contingency plans for import/export and loading features are not tested and evaluated, then it might impact the high availability of the system.				
Recommendation	End-to-End tests should be performed with data import/export/load features into respective databases; test results along with contingency plans should be published in CALT and distributed to appropriate teams for ensuring smooth maintenance of the system. Use the Oracle (COTS) products standard features for importing and exporting of the data.				
Source(s)	**CALT:** doc53234 DSH_PLAN_DataManagement				
IVV Task: OE-12	**Evaluate the results of any volume testing or stress testing.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Verifiability** – Unable to find the Volume and stress testing metrics in CALT.	**5**	**5**	**25**	**High**

Finding Detail	Verify that the results of volume and stress testing will meet nonfunctional performance requirements.
	• External Testing, Performance Stress Test (PST), doc23938 Testing Playbook v0 35 04 19 13
	  • Slide 5
	  • Slide 34
	  • Slide 57 (Test Data Generation and Distribution – Mathematica Test Data Base, Mathematica PST Data, CGI PST Team, QSSI ACA Team, Federal Partners, States)
	  • Slide 58 (Performance Stress Test – June)
	 
	
	  •
	  • Slide 59 (Performance Stress Test – August)
	 

Potential Impact	If volume and stress testing metrics are not available in CALT then performance of the system cannot be determined.				
Recommendation	Provide the volume & stress testing results in CALT to certify that the planned testing actually occurred.				
Source(s)	**CALT:** doc42643 FDSH_R6_Performance_Testing_Results, doc41501 FDSH_PLAN_PTP_R6**,** doc42501 FDSH R6 Perf Test Data – Metrics collected during R6 performance testing				
IVV Task: OE-12		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 2	**Completeness** – Performance testing was executed in isolation due to limited trusted partner's participation.	**5**	**5**	**25**	**High**

Finding Detail	The following document provides details :doc42643 FDSH_R6_Performance_Testing_Results":
	• 100 concurrent users used as baseline
	  ○ Slide 9, Observations
	  ▪ CPU utilization on EWS/SOA-P servers inconsistent – bottlenecks could not be explained.
	  ▪ Connection times and network overheard when testing through public IP inconsistent
	  ○ Slide 10, Issues Encountered
	  ▪ Testing through public IP yielded failures, request timeouts, and inconsistent results
	Due to impact on shared resources (gateways) for IMP Plan Transfer testing, the Team was not able to diagnose this issue or obtain metrics for all services through the public IP**.**				

Potential Impact	If performance testing is executed in isolation (i.e., single & multiple requests are not tracked throughout the entire application between FFE and FDSH, across zones, etc.), then it will be impossible to determine the required bandwidth during peak periods which may result in unscheduled downtimes and ineffective capacity planning.				
Recommendation	Plan performance testing with all affected stakeholders present (including availability of – the Security Team, URS assistance in getting network statistics, trusted partners, etc.) to ensure that a real-world performance testing effort has sufficient bandwidth.				
Source(s)	**CALT:** doc41533 FMPS – Performance Testing Strategy, doc42643 FDSH_R6_Performance_Testing_Results**,** doc42758 FDSH_PM_Performance_Testing_Results				
IVV Task: OE-13	**Evaluate any existing measurement and capacity planning program and will evaluate the system's capacity to support future growth.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Verifiability** – No evidence of a comprehensive Measurement and Capacity Plan in CALT.	**5**	**5**	**25**	**High**

Finding Detail	Capacity planning is one of the most critical responsibilities in the management of an infrastructure. Capacity planning attempts to predict the future load utilization of the System, which could include servers, storage or networks.
Potential Impact	If Measurement and Capacity planning is not documented, then high availability of the system is hard to predict resulting in possible extended downtimes and poor customer experience.
Recommendation	Establish a plan to ensure adequate computing resources are available to handle the projected load and plan for an optimized system during peak and non-peak situations. Ensure hardware and software capacity planning documents are available in CALT.
Source(s)	**CALT:** No Documentation Found

3.5 FDSH SOFTWARE DEVELOPMENT FINDINGS

Table 3-5 FDSH Software Development Findings

IVV Task SD-2	Evaluate the design products for adherence to the project design methodology and standards.	Prob (P)	Impact (I)	Risk Score (P x I)	Risk Level
Finding 1	**Correctness:** Technical Design documents do not address all quality of service (QoS) requirements such as Availability, Accessibility, Integrity, Performance, Reliability, and Regulatory And Security.	**4**	**4**	**16**	**High**
Finding Detail	Technical Design documents do not explain the steps taken to improve the performance of web services. • There is no discussion of the Parsing model to be used and reasons for using a particular xml parser. • There is no discussion about evaluating compressing xml messages. • There is no discussion about why some of the services are synchronous instead of using message queues to improve reliability. • There is no discussion about the using caching and load balances at the application server level.				
Potential Impact	If all the quality of service requirements properties is not addressed in design, then it will lead to poor implementation thus affecting the performance of web services. Also, web services can encounter performance bottlenecks due to the limitations of the underlying messaging and transport protocols.				
Recommendation	Ensure all the quality of service (QoS) properties are addressed in the design documents so that the implementation can be done properly To improve the performance of web services.				

Source(s)	**CALT:** doc54705 FDSH_DEV_TDD_VLP_v33.docx, doc52016 FDSH_RD_BSD_VLP_v33.docx doc54696 FDSH_DEV_TDD_EE.docx doc54694 FDSH_DEV_TDD_APC_T.docx doc54695 FDSH_DEV_TDD_AT.docx doc54698 FDSH_DEV_TDD_IFSV_T.docx doc54699 FDSH_DEV_TDD_MFA_UM_UA.docx doc54700 FDSH_DEV_TDD_RIDP_PI_FARS.docx doc54701 FDSH_DEV_TDD_SSA_Comp.docx doc54702 FDSH_DEV_TDD_VerCurInc_T.docx doc54703 FDSH_DEV_TDD_VerESIMEC.docx doc54704 FDSH_DEV_TDD_VLP_v32_1.docx doc54705 FDSH_DEV_TDD_VLP_v33.docx doc54706 FDSH_DEV_TDD_VerNonESIMEC.docx				
IVV Task: SD-4	**Verify that design requirements can be traced back to system requirements.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Verifiability:** Not all the designs can be traced back to system requirements in CALT.	**4**	**4**	**16**	**High**
Finding Detail	Review of documentations indicated: • Technical Design Documents and BSDs do not have any reference to user stories or CALT artifacts. (doc42858,doc42859,doc42868) • BSDs, BSSs, and DSSs were missing information or marked as “TBD” for security, “Performance Measures “, “Quality of Service” was missing and/or core business mapping missing. (doc42857,doc42867)				
Potential Impact	If design documents cannot be traced back to system requirements, then there may be functionality missing which will impact quality.				
Recommendation	In order to address the above finding: • Ensure that Technical Design Documents and BSDs appropriately reference user stories and CALT artifacts.				
Source(s)	**CALT:** doc42857 FDSH_RD_BSD_EDI_820_FMPS_Payment_Issuers_Service.docx doc42858 FDSH_RD_BSD_Enrollment_999_Reporting.docx doc42859 FDSH_RD_BSD_Exchange_Enrollment.docx doc42867 FDSH_RD_BSD_Verify_Non_ESI_MEC.docx doc42868 FDSH_RD_BSD_Verify_ESI_MEC.docx doc54694 FDSH_DEV_TDD_APC_T.docx doc54696 FDSH_DEV_TDD_EE.docx				

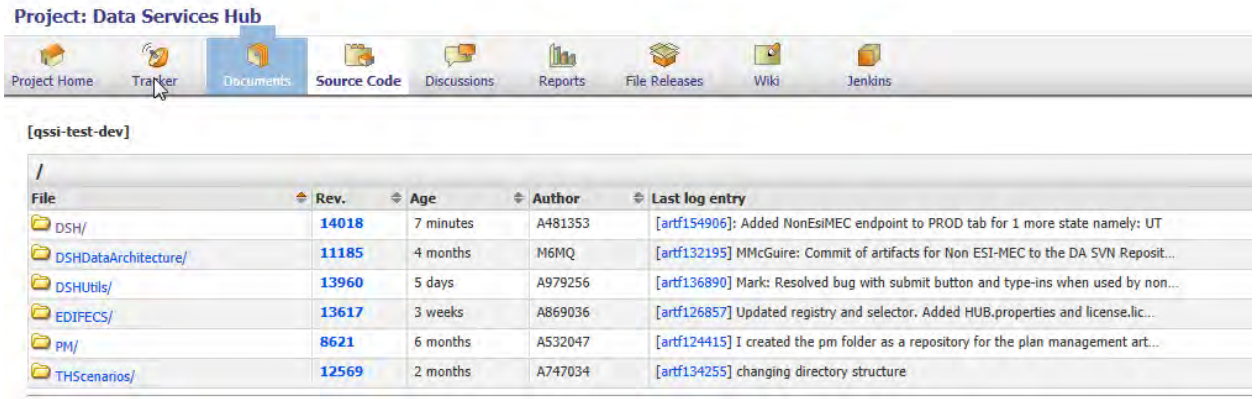
IVV Task SD-4		Prob (P)	Impact (I)	Risk Score (P x I)	Risk Level
Finding 2	**Traceability:** Non-Functional Requirement(s) in the Technical Design Document (TDD) cannot be traced back to the Business Services Design (BSD).	**3**	**3**	**9**	**Moderate**
Finding Detail	As an example, doc54705 p7 Non-Functional Requirement(s) states: "See the VLP v33 BSD". Upon review of referenced document, the requirement could not be located as referenced (doc52016).				
Potential Impact	If the TDD cannot be traced back to the BSD, then production application quality may be jeopardized.				
Recommendation	Ensure that BSDs are traced to TDDs.				
Source(s)	**CALT:** doc54705 FDSH_DEV_TDD_VLP_v33.docx doc52016 FDSH_RD_BSD_VLP_v33.docx				
IVV Task: SD-6	**Perform an evaluation and make recommendations on existing job control and on the process for designing job control.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Completeness:** No evidence of job control in CALT.	**4**	**4**	**16**	**High**
Finding Detail	In doc54696, there is description of 834 X12 batch transactions processes, but no detailed job control process. In doc54701 and doc54702, the requirement for a batch job is described, but no further details were provided to understand how the batch process works. For example: Page 4, doc54701: • "The plan calls for the system to generate and process requests based on individual transactions initiated by the Marketplaces or Medicaid in real-time or near-real time (synchronous); however, the identification of a change in death during the benefit year involves the generation and processing of batch (asynchronous) requests."				
Potential Impact	If detailed job control process is not defined, then there may be a risk that jobs will never be executed, and production application quality will be in jeopardy.				
Recommendation	In order to address the above findings: • Modify the following documents and ensure they include detailed job control processes, in addition the documents should address • Job Frequency • OS level job definitions • Descriptions which provides an understanding for how the job functions • Job parameters				

Source(s)	**CALT**: doc54696 FDSH_DEV_TDD_EE.docx, doc54701 FDSH_DEV_TDD_SSA_Comp.docx doc54702 FDSH_DEV_TDD_VerCurInc_T.docx				
IVV Task: SD-8	**Evaluate batch jobs for appropriate scheduling, timing and internal and external dependencies.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Verifiability:** IV&V team was unable to verify the batch jobs for appropriate scheduling, timing and internal and external dependencies for Release 7.	**2**	**4**	**8**	**Moderate**
Finding Detail	Documents could not be found in CALT for any batch jobs related to software development.				
Potential Impact	If no batch jobs can be evaluated, then there is a risk to the production application when using the batch jobs. There may be defects that cannot be detected.				
Recommendation	Upload documents or scripts for batch jobs into CALT for evaluation.				
Source(s)	**CALT:** No Documentation Found				
IVV Task: SD-9	**Evaluate the appropriate use of OS scheduling software.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Positive Finding:** Tivoli Workload Scheduler is appropriate OS scheduling software for scheduling FDSH jobs.	**N/A**			
Finding Detail	The Tivoli Workload Scheduler (TWS) User Guide provides the process of creating the scheduling objects related to application jobs that needs to be scheduled using Tivoli Dynamic Workload console (TDWC). This software has appropriate level of functions to satisfy user requirements.				
Potential Impact	N/A				
Recommendation	N/A				
Source(s)	**CALT:** doc26944 TWS_FDSH_User Guide_v01.doc				
IVV Task: SD-10	**Verify that job control language scripts are under an appropriate level of configuration control.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Verifiability:** IV&V team was unable to verify whether the batch job control language scripts are under an appropriate level of configuration control for Release 7.	**2**	**4**	**8**	**Moderate**

Finding Detail	There are no documents found in CALT for any job control language scripts that related to the software development for Release 7, so this SOW cannot be verified. Artifacts are found for user stories of previous release- Release 3 and 4 for batch jobs, but none can be found for Release 7 for example: artf105388,artf87043,artf87668,artf95691,artf93357,artf96015,artf97293,artf97295,artf97290,artf97292,artf128420,artf98131,artf97343, artf97342,artf87691,artf87237,artf87238				
Potential Impact	If no batch jobs can be evaluated, then there is a risk to the production application when using the batch jobs. There may be defects that cannot be detected.				
Recommendation	Upload Release 7 documents or scripts for batch jobs into CALT for evaluation.				
Source(s)	**CALT:** artf105388 Simulating the multi Thread for batch Processers not working as expected (Placeholder story) artf87043 Batch File Receiver Component artf87668 As the Hub, determine the structure of batch manifest documents artf95691 Batch orchestration artf93357 Batch Manifest Validator artf96015 Batch Orchestrator (Design) artf97293 Batch Orchestration: BOM Responder artf97295 Batch Orchestration: Batch Processor(s) artf97290 Batch Orchestration: BOM Listener artf97292 Batch Orchestration: Batch Orchestration Module (BOM) artf128420 Batch Framework refactor for IRS artf98131 Batch Orchestration: Testing Activities artf97343 MarkLogic Batch Process Module artf97342 Batch State Schema Definition artf87691 As the Hub, determine the strategy for processing of Batch Files artf87237 As the Hub, delegate a batch file to MarkLogic for processing artf87238 As the Hub, delegate a batch file to Application Zone for processing				
IVV Task: SD-11	**Evaluate and make recommendations on the standards and process currently in place for code development.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Positive Finding:** The software development process for the FDSH project is well documented.	**N/A**			
Finding Detail	The process is well described and provides adequate transparency to understand the software development process for FDSH.				
Potential Impact	N/A				
Recommendation	N/A				

Source(s)	**CALT**: doc27080 FDSH_PROC_Development.docx				
IVV Task: SD-12	**Evaluate the existing code base for portability and maintainability, taking software metrics including but not limited to modularity, complexity and source and object size.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Correctness**: There are a significant number of critical & major code violations in the FDSH code for Release 7.	**4**	**5**	**20**	**High**
Finding Detail	The FDSH Project in CALT has 98 critical and 1,170 Major code violations in Sonar. The critical violations include the following: • Empty If Statement • Security – Array is stored directly • Unconditional If Statement • Correctness – Possible null pointer dereference • Equals Hash Code • Performance – Inefficient use of keySet iterator instead of entrySet iterator • Bad practice – Method may fail to close stream on exception The major violations include the following: • Cyclomatic Complexity • Signature Declare Throws Exception • Avoid Throwing Raw Exception Types • Bad practice – Confusing method names • Boolean Expression Complexity • Malicious code vulnerability – May expose internal representation by incorporating reference to mutable object • Bad practice – Class is Serializable but its superclass doesn't define a void constructor • Exception is caught when Exception is not thrown • Avoid cycle between java packages				
Potential Impact	If the critical and major violations of the code are not fixed, then there will be issues when the application goes to production.				
Recommendation	Ensure FDSH code having critical and major violations in Sonar are reviewed and remediated.				
Source(s)	**CALT/Sonar:** FDSH Project/Dashboard				
IVV Task: SD-12		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 2	**Correctness:** The FDSH code is not easily maintained.	**4**	**4**	**16**	**High**

Finding Detail	For example, defects demonstrated issues related to integration of various services/external systems/handling timeouts, unavailability of services is not optimum. Additionally, design/coding of the application is not properly handling situations like unavailability of external services/systems				
Potential Impact	If Integration of various services/external systems/handling timeouts, unavailability of services is not handled properly, then the application will not function well resulting in bugs and even unavailability of the system.				
Recommendation	Ensure that timeouts from external systems are handled by the code. Ensure design/code can handle unavailability of external systems/sources. Ensure backup or alternate mechanisms are in place to get the data when it is possible.				
Source(s)	**CALT/SVN:** FDSH Project				
IVV Task: SD-13	**Code documentation will be evaluated for quality, completeness (including maintenance history) and accessibility.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Completeness:** Comments in the FDSH code base do not follow best practices and industry standards.	**3**	**4**	**12**	**Moderate**
Finding Detail	Most of the code does not have description, author and revision history. Java Doc comments standards are not consistently followed There are many undocumented APIs.				
Potential Impact	If code comments do not follow best practices, then the maintenance of the code will be very difficult.				
Recommendation	Follow best practices for documenting the code as exhibited in the following URL: (http://www.oracle.com/technetwork/java/javase/documentation/codeconventions-141999.html#385). Document all the APIs.				
Source(s)	**CALT/SVN:** **FDSH Project**				
IVV Task: SD-14	**Evaluate the coding standards and guidelines and the projects compliance with these standards and guidelines. This evaluation will include, but is not limited to, structure, documentation, modularity, naming conventions and format.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Correctness:** FDSH Project does not comply with quality checks defined in the development process document (FDSH_PROC_Development).	**4**	**4**	**16**	**High**

Finding Detail	Section 5.2, FDSH_PROC_Development.docx, "Code Coverage and Quality Check" states: Before checking in any piece of source code, Developers run a Sonar analysis on their local code against the Sonar server and fix any blocker, critical, and major code violations. However, • The FDSH Project has many critical violations as reported by Sonar. • FDSH project code does not follow the Java coding conventions completely. There are many violations of the Java naming conventions for variables, parameters, methods etc. • Even though the code comments are good in general, there are still lots of undocumented APIs.				
Potential Impact	If the critical and major violations of the code are not fixed, then there will be issues when the application goes to production.				
Recommendation	Fix the codes with critical violations in Sonar in CALT. Follow the Java coding conventions including the naming conventions for variables, parameters, methods, etc.				
Source(s)	**CALT:** doc27080 FDSH_PROC_Development.docx **CALT/Sonar** FDSH Project/Dashboard				
IVV Task: SD-15	**Verify that developed code is kept under appropriate configuration control and is easily accessible by developers.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Positive Finding:** FDSH codes are checked in at CALT, and under configuration control, and can be accessed easily by developer.	**N/A**			
Finding Detail	FDSH codes are checked in at CALT, and under configuration control, there are revision numbers, age, and Author for each files. And codes can be downloaded by any authorized developer. Please see the diagram below: 				

Potential Impact	N/A				
Recommendation	N/A				
Source(s)	**CALT:** Data Services Hub				
IVV Task: SD-16	**Evaluate the project's use of software metrics in management and quality assurance.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Verifiability:** There is no evidence that Sonar Violations are being reviewed.	**3**	**3**	**9**	**Moderate**
Finding Detail	CALT Sonar Dashboard for the FDSH project shows 2,003 code violations; there is no evidence that the violations are being reviewed.				
Potential Impact	If the code violations reported by Sonar are not fixed, then it will increase the potential for errors and poor system performance.				
Recommendation	Include Sonar report review as part of the development process and address all the violations.				
Source(s)	**CALT/Sonar:** FDSH Project/Dashboard				
IVV Task: SD-17	**Evaluate the plans, requirements, environment, tools, and procedures used for unit testing system modules.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Verifiability:** No documentation was found for Unit Test plans, requirements, environment, tools, and procedures in CALT.	**4**	**5**	**20**	**High**
Finding Detail	No documentation of Unit testing plans, requirements, environment, tools, procedures, and results were found in CALT for release 7 for FDSH.				
Potential Impact	If Unit Testing plans and results are not found in CALT then the appropriate level of testing may not be able to be verified for the release, including traceability to the functions being developed.				
Recommendation	Provide Unit testing plan, requirements, environment, tools, procedures, and results for release 7 in CALT for review.				
Source(s)	**CALT:** No Documentation Found				
IVV Task: SD-18	**Evaluate the level of test automation, interactive testing and interactive debugging available in the test environment.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Verifiability:** No evidence of test automation, interactive testing and interactive debugging for the test execution in Release 7 for FDSH.	**2**	**4**	**8**	**Moderate**
Finding Detail	No evidence found in CALT to indicate that automated testing, interactive testing and interactive debugging available occurred in the test environment in Release 7 of FDSH.				

Potential Impact	If there is no automated testing used, interactive testing and interactive debugging available in the test environment for a system of this size, then there is a risk that critical functionality may not be tested causing unpredictable results when code is implemented.				
Recommendation	Ensure the results of test automation are published in CALT. Ensure that interactive testing and interactive debugging results are available, so that problems can be addressed appropriately.				
Source(s)	**CALT:** No Documentation Found				
IVV Task: SD-19	**Verify that an appropriate level of test coverage is achieved by the test process, that test results are verified, that the correct code configuration has been tested, and that the tests are appropriately documented.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Completeness:** Low unit test coverage (23.2%) was achieved.	**5**	**4**	**20**	**High**
Finding Detail	These are code coverage for the following modules: FDSH Common ESB – 0% FDSH Common Web – 0% FDSH DAL Common – 13.4% Low unit test coverage indicates that all the modules for Release 7 are not adequately tested.				
Potential Impact	If low unit test coverage occurs, then the complexity and number of defects during testing will increase; therefore, introducing additional risks to successive test cycles.				
Recommendation	Follow test driven development and improve the code coverage.				
Source(s)	**CALT/Sonar:** FDSH Project/Dashboard				

3.6 FDSH SYSTEM AND ACCEPTANCE TEST FINDINGS

Table 3-6 FDSH System and Acceptance Test Findings

IVV Task: ST-1	**Evaluate the plans, requirements, environment, tools, and procedures used for integration testing of system modules.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Completeness:** Testing Milestones status is not updated in the Test Plan.	**2**	**4**	**8**	**Moderate**
Finding Detail	The Testing Milestones status indicates "In Progress" or "Pending Status" in the Test Plan as of October 10, 2013 even though the testing for release 7 has been completed.				
Potential Impact	If the Testing Milestones are not updated in the Test Plan then the user of the Test Plan will not know the correct status of the Testing Milestones causing confusion and critical milestones may be missed.				
Recommendation	Exclude providing the Testing Milestone status as part of the test plan.				
Source(s)	**CALT:** doc54465 R7Sprint20_Test Plan				
IVV Task: ST-1		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 2	**Completeness:** No Test Integration documentation available for releases after sprint 19.	**3**	**4**	**12**	**Moderate**
Finding Detail	No evidence found in CALT of integration testing prepared or executed in the FDSH community folders. The latest evidence of integration testing is from sprint 19 posted to CALT on August 31, 2013.				
Potential Impact	If integration testing is not executed then there is a risk of missing issues that may adversely impact other parts of the system.				
Recommendation	Upload all available Test Integration documentation to the appropriate CALT folder.				
Source(s)	**CALT:** doc43174 FDSH_TST_FFEHUB_IntegrationProfiles_Sprint19V10_4				
IVV Task: ST-1		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 3	**Positive Finding:** Good issues identification and resolution process as evidenced in the "check sum verification case sensitivity issue"	**N/A**			

Finding Detail	Section 5 "Recommendations and Solutions" of the FDSH_Plan_PMPerformance document indicates an issue was discovered that the FDSH MD5 checksum validation is case insensitive causing an integration issue. Artf125921 defect was opened on March 13, 2013 and closed on March 15, 2013 to address the issue.				
Potential Impact	N/A				
Recommendation	N/A				
Source(s)	**CALT:** doc25400 Plan Management Performance test plan; artf125921 PM issues with checksum and bulk DMSClient "FDSH.bulk.webService.save.location" location				
IVV Task: ST-2	**Evaluate the level of automation and the availability of the system test environment.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Verifiability:** No evidence of test automation for the test execution in support of the September 6, 2013 delivery.	**2**	**4**	**8**	**Moderate**
Finding Detail	No evidence found in CALT to indicate that automated testing was invoked to perform testing for the September 6, 2013 delivery of the FDSH code.				
Potential Impact	If there is no automated testing used for a system of this size, then there is a risk that critical functionality may not be tested causing unpredictable results when code is implemented.				
Recommendation	Implement an automated testing tool that can quickly test changes and other parts of the system to ensure new code is working correctly.				
Source(s)	**CALT:** No Documentation Found				
IVV Task: ST-3	**Verify that an appropriate level of test coverage is achieved by the test process, that test results are verified, that the correct code configuration has been tested, and that the tests are appropriately documented, including formal logging of errors**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Positive Finding:** Test Plans are very comprehensive and provide adequate details for the testing.	**N/A**			
Finding Detail	Evidence found in CALT that test plans for the September 6, 2013 delivery are very comprehensive and provide adequate details for testing the release.				
Potential Impact	N/A				
Recommendation	N/A				
Source(s)	**CALT:** doc54465 R7Sprint20_Test Plan				

IVV Task: ST-3		Prob (P)	Impact (I)	Risk Score (P x I)	Risk Level
Finding 2	**Verifiability:** Issues identified in the performance test executed for release 6 and no evidence was found to indicate that subsequent testing was performed to address the problem.	**4**	**5**	**20**	**High**
Finding Detail	• Testing through public IP yielded failures, request timeouts, and inconsistent results. • Account Transfer Schematron processing yielded slow response times and high MarkLogic load • Appzone/Datazone/MarkLogic CPU utilization was not consistent, indicating bursts of request processing				
Potential Impact	If these performance issues are not addressed and retested in subsequent releases then there is a risk of having performance issues when code is executed in production.				
Recommendation	As detailed in the test results: • Needed to understand what was happening when testing over public IP that caused slowdown, failed requests, and connection bottlenecks. • Enhance application log-in where needed to track single requests throughout the entire application, across zones and servers				
Source(s)	**CALT:** doc42643 FDSH_R6_Performance_Testing_Results doc41501 FDSH Release 6 – Performance Test Plan				
IVV Task: ST-3		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 3	**Completeness:** Evidence of Performance Testing is not available for release 7 in CALT; however, status meetings appear to indicate that Performance Testing may have been executed just prior to October 1, 2013 go-live.	**3**	**4**	**12**	**Moderate**
Finding Detail	Full and complete performance testing with the latest functional changes kept being pushed off again and again. It wasn't until the week before the October 1, 2013 go-live that some performance testing was executed and based on the assumption listed in document doc41533, there was no way to be able to do any mitigating actions identified as part of the testing.				
Potential Impact	If performance testing is not executed or performed just before go-live than there is a risk that the project team may not be able to identify potentially fatal performance issues and might not be able to mitigate prior to production implementation.				
Recommendation	Performance testing should be executed with all the functionalities to be released and involving all the interacting systems in order to identify potential issues and mitigate issues prior to production implementation.				
Source(s)	**CALT:** doc41533 FMPS – Performance Testing Strategy				

IVV Task: ST-10	Evaluate interface testing plans and procedures for compliance with industry standards.	Prob (P)	Impact (I)	Risk Score (P x I)	Risk Level
Finding 1	**Verifiability:** FDSH Services tested in isolation.	**3**	**4**	**12**	**Moderate**
Finding Detail	Services were tested in isolation, which does not effectively simulate actual FDSH processing.				
Potential Impact	If testing is done in isolation and does not effectively simulate actual FDSH processing then there is a risk that testing results may be compromised and could potentially cause critical issues and a poor customer experience.				
Recommendation	Need multiple external testing points with enough bandwidth such as Amazon EC2.				
Source(s)	**CALT:** doc42643 FDSH_R6_Performance_Testing_Results				
IVV Task: ST-11	**Acceptance procedures and acceptance criteria for each product must be defined, reviewed, and approved prior to test and the results of the test must be documented. Acceptance procedures must also address the process by which any software product that does not pass acceptance testing will be corrected.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Verifiability:** No evidence of Acceptance Procedure and Acceptance Criteria found in CALT.	**3**	**4**	**12**	**Moderate**
Finding Detail	Although some integration data profiles were identified, no Acceptance Procedures and/or Acceptance Criteria documentation for FDSH was found in CALT.				
Potential Impact	If Acceptance Procedures and Acceptance Criteria are not available for testing and integrating with FDSH than there is a risk that integration issues may be encountered in production.				
Recommendation	Provide the appropriate Acceptance Procedures and Acceptance Criteria documentation and store in CALT.				
Source(s)	**CALT:** doc43174 FDSH_TST_FFEHUB_IntegrationProfiles_Sprint19V10_4				
IVV Task: ST-11		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 2	**Process Deviation:** No acceptance testing documentation found in CALT.	**3**	**4**	**12**	**Moderate**
Finding Detail	Acceptance testing documentation was not found in CALT. No acceptance testing documentation was provided upon a document request. No evidence found in CALT of gate reviews held prior to acceptance testing.				
Potential Impact	If the government does not have an objective, independent review of acceptance testing, then the government will not be able to take corrective action over the unknown numbers of incomplete, incorrect, inconsistent, inaccurate test procedures, and acceptance criteria.				

Recommendation	Prepare acceptance criteria at the beginning of each sprint. Review acceptance criteria at the end of each sprint. Document acceptance criteria in CALT				
Source(s)	**CALT:** No Documentation Found				
IVV Task: ST-12	**Verify that appropriate acceptance testing based on the defined acceptance criteria is performed satisfactorily before acceptance of software products.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Verifiability:** No evidence was found of UAT plan or results for release 7.	**4**	**4**	**16**	**High**
Finding Detail	No evidence of UAT plans or results were found in CALT for release 7 for the FDSH Integration.				
Potential Impact	If UAT plans and results are not found in CALT then the appropriate level of testing may not be able to be verified for the release, including traceability to the functions being developed.				
Recommendation	Provide UAT plans and results in CALT for review.				
Source(s)	**CALT:** No Documentation Found				
IVV Task: ST-15	**Review and evaluate implementation plan.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Completeness:** No evidence was found of a formal implementation guide for the September 6, 2013 delivery.	**3**	**4**	**12**	**Moderate**
Finding Detail	No evidence was found of a formal implementation guide for the September 6, 2013 delivery; however, the Operational Readiness Review (ORR) Checklist should contain adequate guidance to implement the delivery.				
Potential Impact	If a formal implementation guide does not exist than there is a risk that critical implementation step may be missed or out of order causing unnecessary delays and issues with the implementation.				
Recommendation	Develop a formal implementation guide and store in CALT.				
Source(s)	**CALT:** doc54521 CM Readiness Review Checklist Sprint21 Release7 doc49468 CM Readiness Review Checklist Sprint20 Release6				

3.7 FDSH DATA MANAGEMENT FINDINGS

Table 3-7 FDSH Data Management Findings

IVV Task: DM-1	Evaluate CMS's existing and proposed plans, procedures and software for data conversion.	Prob (P)	Impact (I)	Risk Score (P x I)	Risk Level
Finding 1	**Completeness:** There is no detailed information on data conversion.	2	4	8	Moderate
Finding Detail	On page 32 5.3 Data Conversion only discusses the following: The Team typically achieves data conversion by one of the following methods: • XSLT style sheets that convert one XML format to another • Java manipulation of XML data • MarkLogic conversion via Xquery or XSLT				
Potential Impact	If there is no detailed information provided, then there is no plan to accomplish data conversion having significant downstream impacts to all web services transactions affecting all insurer data feeds and federal partner interfaces.				
Recommendation	Update the document with specific information which addresses data conversion program requirements.				
Source(s)	**CALT**: doc53260 FDSH_DES_SDD.docx				
IVV Task: DM-5	**Evaluate new and existing database designs to determine if they meet existing and proposed system requirements.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Completeness:** The local MarkLogic database configuration guide doesn't contain sufficient details to understand how the database configuration will be achieved. In addition the document isn't consistent with CMS document formats.	4	4	16	High
Finding Detail	The MarkLogic database configuration guide isn't a comprehensive guide. The guide lacks details a DBA needs to configure the MarkLogic Database. For example: the schema, forest, and server cluster information are not discussed in the guide. This document doesn't capture the following details to be consistent with CMS document formats: • Version Number • Document Title • Revision Table and Number • Author Name				

Potential Impact	If the MarkLogic configuration guide isn't comprehensively detailed then an inadequate configuration may be produced significantly impacting database performance and may result in downstream impacts on processes/activities/applications/web services transactions which depend on MarkLogic databases. If inconsistent document formatting exists then document maintainability will be impacted.				
Recommendation	Update the document with detailed instructions on how the MarkLogic database should be configured and follow the CMS file format to provide the information mentioned above. Refer to MarkLogic's Administrator's Guide and other applicable instructions as a best practice to develop a comprehensive configuration installation guide. The schema, forest and server clusters should be reflected in the configuration details. Lastly, ensure the configuration guide addresses all applicable system requirements associated with FFM functionality.				
Source(s)	**CALT:** doc10008 Local MarkLogic Setup Guide				
IVV Task: DM-5		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 2	**Completeness:** FDSH_PLAN_DataManagement (doc53234) and FDSH_DES_SDD (doc53260) documents do not provide adequate database design details for FDSH.	**3**	**3**	**9**	**Moderate**
Finding Detail	Doc53260 discusses database design in section 5.2; however it doesn't provide adequate details. The rationale is on Page 29, however it should describe the design of all database management system (DBMS) files and non-DBMS files associated with the Hub. For example, the document discusses the following "The Federal FDSH is actually more concerned with Web services and the exchange of information between systems and government agencies." Again, the example doesn't address or describe the actual DB design as it relates to web services. The FDSH_PLAN_DataManagement doesn't comprehensively address database design. The lack of details won't enable appropriate data management activities i.e. data quality, data auditability, persistent data across business areas, security & privacy, schema management etc…				
Potential Impact	If the database design is not adequately detailed, then database maintainability may significantly be impacted.				
Recommendation	Update doc53234 or doc 53260 with appropriate database design details. As a DMBOK best practice, a comprehensive database design approach should enable appropriate data management activities e.g. data quality, data auditability, persistent data across business areas, security & privacy, schema management.				
Source(s)	**CALT:** doc53234 FDSH_PLAN_DataManagement.docx; doc53260 FDSH_DES_SDD.docx				
IVV Task: DM-6	**Recommend improvements to existing designs to improve data integrity and system performance.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Completeness:** FDSH_DES_SDD (doc53260) does not provide sufficient details to understand how the design addresses performance, hardware, software, security and internal communications.	**4**	**4**	**16**	**High**

Finding Detail	On Page 36, points to: https://calt.cms.gov/sf/docman/do/listDocuments/projects.FDSH/docman.root.release_notes.development_artifacts_by_release for detailed design for performance, hardware, software, security and internal communications. When this link is selected, it opens a folder in CALT. Under this folder, you can find release folders and sprint folders, however there are no detailed designs for performance, hardware, software, security and internal communications.				
Potential Impact	If the FDSH _DES_SDD document lacks adequate design details to understand how performance can be optimized for existing software, hardware and security configurations then it will be difficult to troubleshoot and resolve problems.				
Recommendation	Update doc53260 FDSH_DES_SDD.docx to include detailed design information which addresses performance, hardware, software, security and internal communications. The details should describe the engineered design with sufficient traceability to technical/business requirements to ensure performance satisfies architectural specifications.				
Source(s)	**CALT:** doc53260 FDSH_DES_SDD.docx				
IVV Task: DM-6		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 2	**Completeness**: The Data Quality & Data Verification and Validation approach is incomplete.	**4**	**4**	**16**	**High**
Finding Detail	It's not evident the plan comprehensively addresses data quality. For example: • Data quality requirements are not mentioned therefore, traceability to data quality can't be determined. • The data quality approach doesn't address roles and responsibilities involved in data quality activities. • The data quality approach doesn't identity data quality metrics. • It's not clear how data quality metrics will/can be consistently captured. • Data cleansing activities are not addressed. • Data reduction activities are also not mentioned. Example: A strategy focused on data reduction should address closing obsolete transactions.				
Potential Impact	If data quality and data verification/validation plans are not comprehensively detailed, then: • Inadequate data quality metrics may not address data deficiencies as code is promoted in successive environments. • The program may be unable to measure data quality which may hinder improvement activities. • Application functionality may fail which will increase rework to resolve defects.				

Recommendation	Update the plan to comprehensively achieve data quality. The following recommendations are based on the DMBOK: • Identify data quality requirements and ensure data quality activities are traceable to them • Develop an approach to harmonize, extract and measure data quality across all master data elements and data environments. • Create a Data Quality team that will monitor data quality across all environments including production. • Identify a data steward responsible for data coordination activities. • Develop a RACI which integrates into the larger data management approach. • Develop an approach to identify data quality metrics and thresholds to support business capabilities and data fitness for use. • Categorize data quality metrics – e.g. Data Type, Data Domain Compliance, etc. • Develop an approach for data quality across both master and transactional data. • Develop an approach to establish a root cause analysis process to include data quality criteria, stage gates and data decision making processes. • Develop an approach to data cleansing. • Develop an approach to data reduction (closing obsolete transactions, reducing new transactions) • Develop an approach to data verification planning. • Develop an approach to stakeholder and SME involvement. • Data verification and validation activities must be an on-going program and traceable to code promotion deployment milestones				
Source(s)	**CALT:** doc53234 FDSH_PLAN_DataManagement				
IVV Task: DM-8	**Evaluate the project's process for administering the database, including backup, recovery, performance analysis and control of data item creation.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Positive Finding:** FDSH_IMP_OMM.docx (doc26320) provides complete and correct database backup processes.	**N/A**			
Finding Details	The IV&V team found that Oracle and MarkLogic database backup procedures are identified and complete.				
Potential Impact	N/A				
Recommendation	N/A				
Source(s)	**CALT:** doc26320 FDSH_IMP_OMM.docx				
IVV Task: DM-8		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 2	**Completeness:** Oracle and MarkLogic database administration procedures are incomplete.	**3**	**3**	**9**	**Moderate**
Finding Detail	In FDSH_IMP_OMM.docx (doc26320), Chapter 5 Data and Database Administration (DBA), there are steps for database backup and FDSH DBA roles, but no information provided for local recovery, performance analysis and control of data item creation.				

Potential Impact	If no detailed database administration procedures are in place for local recovery then the DBA won't have procedures to reference to accomplish database recovery or address performance issues.				
Recommendation	Update docc26320 with procedures for database recovery, performance analysis, user role security controls and creation of database objects.				
Source(s)	**CALT:** doc26320 FDSH_IMP_OMM.docx				
IVV Task: DM-8		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 3	**Completeness:** Inadequate resource allocation i.e. one resource is allocated to perform all DBA tasks.	**3**	**3**	**9**	**Moderate**
Finding Detail	In doc26320, pg. 44 Table 16 – PM Database Administration Team, only one personnel is listed.				
Potential Impact	If there is only one person assigned to perform all DBA tasks, and there is no assigned backup then this presents a potential risk that all DBA related tasks may not be completed or if performed may fail to meet SLA (Service Level Agreement) DB availability requirements.				
Recommendation	Add more resources to the DBA team.				
Source(s)	**CALT:** doc26320 FDSH_IMP_OMM.docx				
IVV Task: DM-8		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 4	**Completeness**: FDSH Disaster Application Backup procedures; Information Systems Backup; Information Systems Recovery & Reconstitution are incomplete.	**4**	**4**	**16**	**High**
Finding Detail	Appendix L "How to bring the Federal FDSH Application Back up in a Disaster – doesn't capture program business requirements… For example, the procedures should address timing, SLA performance requirements and troubleshooting scenarios. Incremental backup activities don't appear to be comprehensive. For example when a restore is required, who are the contacts for each of the federal partners affected? There is no RACI that captures details below organizational/department assignment. Backup/restore requirements do not demonstrate traceability to service management requirements. Periodic evaluation/review of the procedures are not included to ensure backup/restore processes remain current and reflect business objectives and program risk mitigation strategies.				
Potential Impact	If the FDSH Disaster Application Backup procedures, Information Systems Backup, Information Systems Recovery & Reconstitution are incomplete then restoration activities may be extended (i.e. take longer than necessary) impacting the user community and partners who rely on the hub.				

Recommendation	Update the plan with: • Additional details addressing SLA requirements and performance requirements • Incremental backup troubleshooting scenarios • Notification activities • Periodic evaluation/review of the procedures • RACI				
Source(s)	**CALT:** doc48809 FDSH_SEC_ISCP.docx				
IVV Task: DM-8		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 5	**Correctness**: 4 Week backup history may not meet program requirements.	**4**	**4**	**16**	**High**
Finding Detail	4 weeks of history is being stored on tapes but may not be sufficient. The tactical steps involved in tape restoration and notification activities are not sufficiently described to understand how the backup will satisfy program requirements.				
Potential Impact	If a 4 week backup history may not meet program requirements or other mandated CMS regulations, then: • Restoration activities may take longer than planned. • History on backup tapes may be inadequate or fail to satisfy history requirements.				
Recommendation	Update the document to include recovery/backup history requirements and also includes contact information for each program partner/contractor involved in restoration activities. Include a provision for periodic reviews as a process improvement activity.				
Source(s)	**CALT:** doc48809 FDSH_SEC_ISCP.docx				
IVV Task: DM-8		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 6	**Verifiability**: pmTransferReport_2013810-100.255528 (doc45955) MarkLogic report does not contain a sufficient number of report attributes for complete audit of data.	**4**	**3**	**12**	**Moderate**
Finding Detail	The PM MarkLogic transfer report doesn't contain a sufficient number and diversity of attributes to provide confidence in the auditability of all data and transaction activities involved in the PM transfer process. For example it only contains the following attributes: column name, service, operation, from and to. The report is blank i.e. it has no data.				
Potential Impact	If the PM Transfer report isn't comprehensively detailed with appropriate attributes to enable auditability then production issue diagnosis/resolution and/or data restoration activities may be impeded.				
Recommendation	Review the report design and intended use. The report should minimally address all data auditability requirements. Ensure CMS leadership has signed off on the final design and data capture.				
Source(s)	**CALT:** doc45955 pmTransferReport_2013810-100.255528.csv				

3.8 FDSH OPERATIONS OVERSIGHT FINDINGS

Table 3-8 FDSH Operations Oversight Findings

IVV Task: OO-5	Evaluate operational plans and processes.	Prob (P)	Impact (I)	Risk Score (P x I)	Risk Level
Finding 1	**Completeness:** The FDSH SSP is incomplete.	3	3	9	**Moderate**
Finding Detail	MITRE evaluated the FDSH SSP v .2 in June 2013. At that time, there were: 131 items that were partially compliant and 63 items that were "Not Addressed." IV&V used a sampling technique of checking every tenth item to determine whether these items had been addressed in the SSP in CALT that was labeled as "Final." The IV&V findings are: • In 7/13 cases (53%), the items previously identified as "partial" were still not addressed. • In 5/6 cases (83%), the items previously identified as "not addressed" were still not addressed.				
Potential Impact	If this SSP (doc53567) was the final SSP, then there are a significant number of controls that are not addressed, which may result in security breaches / incidents.				
Recommendation	Implement the security controls to reduce the exposure to security risk.				
Source(s)	**CALT:** doc53567 doc47376				
IVV Task: OO-5	**Evaluate operational plans and processes.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 2	**Completeness:** Multiple tasks in CDM Master Schedule (doc43677) have not been finished on due date	**4**	**4**	**16**	**High**

Finding Detail	The following tasks are taken from the project schedule: • Task ID 1 1 Reference Models (48% finished, Due date October 8, 2013, Duration: 77 days) • Task ID 38 CIEM 2.2 (4% finished, Due date August 14, 2013, Duration: 75 days) • Task ID 75 2 Information Exchange Models (66% finished, Due date October 10, 2013, Duration: 159 days) • Task ID 63 2-2 Customizations (56% finished, Due date October 21, 2013, Duration: 57 days) • Task ID 119 2-3 Documentation (63% finished, Due date October 1, 2013, Duration: 145 days) • Task ID 160 3 Usage Documentation (84% finished, Due date October 10, 2013 Duration: 145 days) • Task ID 193 4 Reference Model Maintenance Documentation (50% finished, Due date October 2, 2013 Duration: 115 days) • Task ID 241 5 Options Papers (57% finished, Due date October 2, 2013)				
Potential Impact	If the schedule is not an accurate reflection of development activities then schedule variance will continue to increase significantly impacting the quality and completeness of code drops, testing, data management and other quality activities.				
Recommendation	Update doc43677 and review the integrated master schedule and coordinate with CMS/contractor task leads to ensure impacts are defined wherever tasks have the potential to affect integration activities and other critical milestones.				
Source(s)	**CALT:** doc43677 CDM Master Schedule.mpp (As of October 4, 2013 update)				
IVV Task: OO-5		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 3	**Completeness:** Multiple tasks in FDSH_Planning_Schedule (doc31409) have not been finished on due date	**4**	**4**	**16**	**High**
Finding Detail	The following tasks are taken from the project schedule: • Task ID 548 MEDICAID/CHIP END TO END TESTING COMPLETE (ADD) (0% finished, Due date September 30, 2013, Duration: 1 days) • Task ID 999 OPM END TO END TESTING COMPLETE (ADD) (0% finished, Due date September 30, 2013, Duration: 1 days) • Task ID1169 FINALIZE ICD (ADD) (0% finished, Due date October 4, 2013, Duration: 1 days) • Task ID1547 HUB APPLICATION MONITORING (ADD) (97% finished, Due date September 30, 2013, Duration: 3.75 Months) • Task ID1652 DRAFT SCA REPORT REVIEW (0% finished, Due date October 1, 2013, Duration: 1 days) • Task ID1657 IMPLEMENTATION ACTIVITIES FOR DAY1(ADD) (69% finished, Due date September 28, 2013, Duration: 4 days) Task ID1682 INFRASTRUCTURE TASKS (30% finished, Due date September 28, 2013, Duration: 4 days)				
Potential Impact	If testing tasks are not completed on time, then data quality, data integration and associated dependencies may be significantly impacted across environments.				

Recommendation	Review the integrated master schedule and coordinate with CMS/contractor task leads to ensure impacts are defined wherever tasks have the potential to affect integration activities and other critical milestones.				
Source(s)	**CALT:** doc31409 FDSH_Planning_Schedule.mpp (as of October 1, 2013)				
IVV Task: OO-6	**Evaluate implementation of the process activities including backup, disaster recovery and day-to-day operations to verify the processes are being followed.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Consistency:** Disaster Recovery in the FDSH ISCP document isn't consistent with CCIIO Resource Allocations by Project – ECPE Cloud 20130517.pdf.	**4**	**4**	**16**	**High**
Finding Detail	Page 1 of doc48809 states "The DR site infrastructure consists of the same components as the primary site. During normal operations, the DR site servers update with changes made to the primary site hosts. Data replicates continually to the DR site to maintain a working copy of the database. The servers in the DR site are available and maintained as production hosts." But based CCIIO Resource Allocations by Project – ECPE Cloud 20130517.pdf, the DR site for FDSH has not been setup yet. IV&V presented the following question to Terremark on May 23rd, 2013 during an interview: "Why does the Disaster Recovery Failover site not provide enough space to support failover and recovery", Terremark's response "the decision was made by the project owner." The figure below demonstrates there are no VM servers set up at the DR site for FDSH.				

Date 17-May-13

Processor Size (GHz) - Culpeper 3.457
Processor Size (GHz) - Miami 2.925

	CCIIO Cloud Resource Allocations by Project (as provisioned)							
	Culpeper				Miami (DR Failover)			
	Virtual Machines (VMs)	Processors (#VPUs)	Memory (GB)	Storage (GB)	Virtual Machines (VMs)	Processors (#VPUs)	Memory (GB)	Storage (GB)
CALT Project Total	13	74	240	7050	6	10	18	794
CMMI Project Total	9	36	144	2240	0	0	0	0
CMSNet Project Total	3	4	28	275	0	0	0	0
DSH Project Total	171	684	2126	33320	0	0	0	0
ECWS Project Total	66	146	449	10529	0	0	0	0
EIDM Project Total	67	310	700	13540	0	0	0	0

Potential Impact	If a DR Failover site is not the hot backup site (i.e. all files in the primary site backup to failover over in a timely manner), then it will be impossible to recover when the primary site is down.				
Recommendation	Review all DR failover requirements. Update all processes and procedures to address synchronization of primary site data files with failover site data files to ensure the failover site becomes the new primary when/if the primary site is lost. The DR Failover site should be a hot backup site.				
Source(s)	**GTL:** CCIIO Resource Allocations by Project – ECPE Cloud 20130517.pdf **CALT:** doc48809-FDSH_SEC_ISCP.docx				
IVV Task: OO-6		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**

Finding 2	**Completeness:** There is no Disaster Recovery (DR) site for FDSH.	**2**	**5**	**10**	**Moderate**
Finding Detail	• No DR status was provided during the pre and post-Deployment meetings even though they were part of the checklists. • No apparent CALT documentation provides the status of the HP DR site, which was supposed to be ready by Oct. 1. • The current FDSH Contingency Plan (in CALT) still states that the DR is at Terremark. • However, according to the FDSH SCA, there is no DR site for FDSH, and Terremark does not have the components needed to provide DR for FDSH. • The FDSH SCA also states "Though Terremark backs up all data to the Miami facility; there is no agreement with CMS to recover the private cloud in the event of a disaster effecting the Herndon facility." • The FDSH SCA also states that the FDSH was not designated as a mission-critical system even though the Recovery Time Objective (RTO) is 4 hours (which is categorized by NIST as "High"). Thus, CMS is not following NIST.				
Potential Impact	If a disaster occurs during this time of no coverage, then the following may occur. • The State-Based Marketplaces will not be able to perform automated verifications, etc. as required by federal law. • The Federally-Facilitated Marketplaces will not be able to perform automated verifications, etc. as required by federal law. • CMS will gain further bad press.				
Recommendation	• Establish a DR site ASAP. • Document a contingency plan for recovery during the period that there is no DR site. • Ensure SBMs have contingencies in place for operating should a disaster wipe out FDSH. • Establish NIST controls as a standard.				
Source(s)	**Email:** CMS Marketplace Checklist – 9-24-13_v10, p. 59; Pre-Deployment ORR PRR_Meeting Capture_09212013, p. 7. **CALT:** doc53047, doc48809, doc53567				

APPENDICES

APPENDIX A: ACRONYMS

Acronyms used in this document are listed below.

Acronym	Description
ACA	Affordable Care Act
ANSI	American National Standards Institute
API	Application Program Interface
ATO	Authority to Operate
BSD	Business Service Definition
BSS	Business Service Specifications
CALT	Collaborative Application Lifecycle Tool
CASE	Computer-Aided Software Engineering
CCB	Change Control Board
CCIIO	Consumer Information & Insurance Oversight
CDM	Canonical Data Model
CDN	Content Delivery Network
CFACTS	CMS FISMA Control Tracking System
CFR	Code of Federal Regulations
CHIP	Children's Health Insurance Program
CIISG	Consumer Information & Insurance Systems Group
CMMI	Capability Maturity Model Integration
CM	Configuration Management
CMP	Change Management Plan
CMS	Centers for Medicare & Medicaid Services
COA	Class of Admission
COBIT	Control Objectives for Information and Related Technology
COI	Critical Operational Issues
COOP	Continuity of Operations Plan
CoRB	Content-Reprocessing in Bulk
COTS	Commercial-Off-The-Shelf
CPU	Central Processing Unit
CR	Change Request
CRM	Customer Relationship Management
DAL	Data Access Layer
DB	Database
DBA	Data Base Administrator
DDI	Design, Development, and Implementation
DDR	Detailed Design Review
DM	Data Management
DMBOK	Data Management Body of Knowledge
DOD	Department of Defense
FDSH	Data Services Hub
DW	Data Warehouse
ECM	Enterprise Canonical Model
EE	Eligibility and Enrollment
E&E	Eligibility and Enrollment
EMF	Eclipse Modeling Framework
EOY	End of Year

Acronym	Description
FDDR	Final Detailed Design Review
FMPS	Federal Marketplace Program System
FFE	Federally-Facilitated Exchange
FFM	Federally Facilitated MarketPlace
FIPS	Federal Information Processing Standard
FM	Financial Management
GTL	Government Task Lead
HHS	Health and Human Services
HIX	Health Insurance Exchange
HIPAA	Health Insurance Portability and Accountability Act
HIOS	Health Insurance Oversight System
HL7	Health Level 7
HPQC	Hewlett-Packard Quality Center
HTML	Hyper Text Markup Language
IaaS	Infrastructure as a Service
ICD	Interface Control Document
IEEE	Institute of Electrical and Electronics Engineers
IHE	Integrating the Healthcare Enterprise
IMS	Integrated Master Schedule
IP	Internet Protocol
IPT	Integrated Project Team
IRS	Internal Revenue Service
ISCP	IS Contingency Plan
IT	Information Technology
ITIL	Information Technology Infrastructure Library
IV&V	Independent Verification and Validation
JVM	Java Virtual Machine
MDM	Master Data Management
MDA	Model Driven Architecture
MDM	Master Data Management
MEC	Minimum Essential Coverage
MIDAS	Multidimensional Insurance Data Analytics System
N/A	Not Applicable
NCPDP	National Council for Prescription Drug Programs
NHIN	National Health Information Network
NIST	National Institute of Standards and Technology
NLM	National Library of Medicine
OLTP	On Line Transaction Processing
OE	Operating Environment
OIS	Office of Information Services
OO	Operations Oversight
OPM	Office of Personnel Management
ORR	Operational Readiness Review
OS	Operating System
PaaS	Platform as a Service
PISP	Policy for the Information System Program
PBR	Project Baseline Review
PM	Plan Management
PMO	Project Management Office
PMD	Programming Mistake Detector

Acronym	Description
PMBOK	Project Management Institute's Project Management Body of Knowledge
PMP	Project Management Plan
POC	Point Of Contact
PPACA	Patient Protection Affordable Care Act
PRA	Paperwork Reduction Act
PST	Performance Stress Testing
QA	Quality Assurance
QAP	Quality Assurance Plan
QASP	Quality Assurance Surveillance Plan
QC	Quality Control
QCP	Quality Control Plan
QHP	Quality Health Plan
QM	Quality Management
QMP	Quality Management Plan
QSSI	Quality Software Services, Inc.
QTP	Quick Test Pro
RAM	Random Access Memory
RBAC	Role Based Access Control
REQMP	Requirements Management Plan
RIA	Rich Internet Applications
RM	Requirements Management
ROM	Rough Orders of Magnitude
RMP	Risk Management Plan
RR	Requirements Review
RTM	Requirements Traceability Matrix
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SAS	Statistical Analysis System
SCA	Security Control Assessment
SD	Software Development
SDD	Software Design Document
SDLC	System Development Life Cycle
SEI	Software Engineering Institute
SLA	Service Level Agreement
SOAP	Simple Object Access Protocol
SOW	Statement of Work
SQL	Structured Query Language
SSA	Social Security Administration
SSF	Single Streamlined Form
SSP	System Security Plan
ST	System Testing
SVN	Subversion
TBD	To Be Determined
TDD (1)	Technical Design Document
TDD (2)	Test Driven Design
TDS	Trusted Data Source
TPGSI	TurningPoint Global Solutions
TRA	Technical Reference Architecture
TRR	Test Readiness Reviews
TWS	Tivoli Workload Scheduler

Acronym	Description
UAT	User Acceptance Testing
UI	User Interface
UML	Unified Modeling Language
URR	Unit Readiness Review
UT	Unit Test
V&V	Verification and Validation
VA	Veterans Administration
VDC	Virtual Data Center
VHA	Veterans Health Administration
VLP	Verify Lawful Presence
VRR	Validation Readiness Review
VM	Virtual Machine
W3C	World Wide Web Consortium (W3C)
WSDL	Web Services Description Language
XA	Extended Architecture
XCC	XML Counterbase Connector
XLC	Expedited Life Cycle
XML	Extensible Markup Language
XSD	XML Schema Definition
XSLT	Extensible Stylesheet Language Transformations

APPENDIX B: INTERVIEWS AND MEETINGS

Table B-1 Interviews & Meetings

Name	Functional Area	Date
[redacted]	Remedy Discussion	7/26/2013
[redacted]	JOLT 3 Demo meeting	7/31/2013
[redacted]	EE UAT Kick Off	8/1/2013
[redacted]	Account Lite UAT	8/2/2013
[redacted]	JIRA Demo	8/30/2013
[redacted]	FMPS Pre-Flight - Operational Readiness Review and Production Readiness Review	9/20/2013
[redacted]	Marketplace IT PRR - Post Deployment	9/25/2013
[redacted]	Daily Morning Production Support Status Call	Daily
[redacted]	FMPS Prod-Dev-Testing Morning Meeting	Daily
[redacted]	Triage UAT Defects	Daily
[redacted]	PMO Weekly Meeting	Weekly
[redacted]	FMPS IV&V Weekly Status Meetings	Weekly
[redacted]	Internal Testing Milestones	Weekly
[redacted]	Marketplace IT CCB Meetings	Twice Weekly
[redacted]	Executive Status Meeting	Monthly

APPENDIX C: REVIEWED DOCUMENTATION

Table C-1 Reviewed Documentation

Document Element #	Document ID #	Document/Information Received	Source
D01	doc51976	EE_R7.0.1_UserGuide	CALT
D02	doc28140	Tivoli Workload Scheduler (TWS) training 1	CALT
D03	doc33123	PM_R6_RatingModule_UserGuide	CALT
D04	doc33123	PM_R6_RatingModule_UserGuide	CALT
D05	doc3141	HHS -Federal Exchange Statement of Work	CALT
D06	doc4375	FFE Requirements Management Plan	CALT
D07	N/A	FFE Traceability Presentation for IV&V 07/31/12	GTL
D08	N/A	Business Architecture Baseline Presentation for IV&V, 7/31/2012	GTL
D09	N/A	Business Architecture Baseline Reconciliation CALT & Process Updates, 06/12/2012.	GTL
D10	N/A	IV&V Meeting with CMS Management, September 17, 2012	Meeting
D11	N/A	Notes from CCIIO Requirements Meeting 090612, v3	Meeting
D12	N/A	conducted on July 12, 2012	Interview
D13	doc46152	EE_R7.0_SRD_RTM_Draft	CALT
D14	doc46016	CBS-EXCH-EE-211_Eligibility_Support_Desktop_Scan_Mailroom_Documents_BSD	CALT
D15	doc46005	EE_R7.0_BusinessServiceSpecifications	CALT
D16	doc46006	EE_R7.0_DataServiceSpecifications	CALT
D17	doc46008	EE_R7.0_ServiceSequenceDiagrams	CALT
D18	doc35708	CBS-EXCH-EE-208_Plan_Compare_Screening_Questions_BSD	CALT
D19	doc34580	CBS-EXCH-EE:114 Process Plan Selection Release 3	CALT
D20	artf149831 thru 149835	FFM allows CSR to view Authorized Representative Information	CALT
D21	artf151100 thru 151120	DEV Person Matching	CALT
D22	artf151047 thru 151073	DEV Recalculate APTC	CALT
D23	artf34838; artf41499	FFM allows CSR to view Authorized Representative Information	CALT
D24	artf34838; artf41499	Notify Issuer of Intent to Disenroll	CALT
D25	artf150336	Cancellation	CALT
D26	artf150342	Termination	CALT
D27	artf96183	Issuer Response - Exchange	CALT
D28	doc46152	EE_R7.0_SRD_RTM_Draft	CALT
D29	doc46153	EE_R7.0_ReleasePlan	CALT
D30	doc46005	EE_R7.0_BusinessServiceSpecifications Touching Bases--delayed	CALT

		opening for students	
D31	doc46012	EE_R7.0_UISpecifications	CALT
D32	artf149831 thru 149835	FFM allows CSR to view Authorized Representative Information	CALT
D33	artf151100 thru 151120	DEV Person Matching	CALT
D34	artf151047 thru 151073	DEV Recalculate APTC	CALT
D35	artf151089 thru 151099	Basic Linking between My Account and Ind. Application	CALT
D36	artf150336	View Artifact	CALT
D37	artf150342	View Artifact	CALT
D38	artf96183	View Artifact	CALT
D39	N/A	CGI, MITRE held on 4/11/2013	Interview
D40	N/A	GENOVA held on 3/13/2013	Interview
D41	doc4375	FFE Requirements Management Plan Section 5.1.2 FFE / FDSH Requirements Manager	CALT
D42	doc13710	Plan Management_Issuer Application_v64_Working	CALT
D43	doc10822	PM Process Model v61 08202012	CALT
D44	doc5115	PM_Benefit Data Collection_Sprint4_Epic2	CALT
D45	doc2547	PM_Initial Issuer Application Collection_Sprint2_Epic4_OLDER VERSION	CALT
D46	doc6795	FM (Federal) - Process Model v56.vsd	CALT
D47	N/A	CMS Weekly Status – 4Corner – April 22, 2013 (HHS-CMS Issues Log)	GTL
D48	doc7475	ECloud Backup Process Document 05_08_2012	CALT
D49	doc12881	Backup and Restore Services procedures	CALT
D50	doc12885	OM Manual eCAP	CALT
D51	doc12859	CFACTS CSP4PaaS SSP	CALT
D52	doc42643	FDSH_R6_Performance_Testing_Results	CALT
D53	doc41501	FDSH Release 6 - Performance Test Plan	CALT
D54	doc25400	FDSH_PLAN_PMPerformance_v1_0_D	CALT
D55	doc41500	FDSH_Plan_Transfer_Performance_Testing_Results	CALT
D56	CALT Project: Data Services Hub\Trackers	List Trackers and Planning Folders	CALT
D57	doc53234	FDSH_PLAN_DataManagement	CALT
D58	doc12880	PaaS VM Software Components	CALT
D59	doc12381	FFE_HTD	CALT
D60	doc11023	CSP4IaaS C&A Artifacts Update 091212	CALT
D61	doc41501	FDSH_PLAN_PTP_R6	CALT
D62	doc42501	FDSH R6 Perf Test Data - Metrics collected during R6 performance testing	CALT
D63	doc41533	FEPS - Performance Testing Strategy	CALT
D64	doc19855	FDSH_PM_Performance_Testing_Results	CALT
D65	doc53260	FDSH_DES_SDD	CALT

D66	doc26320	FDSH_IMP_OMM	CALT
D67	doc54705	FDSH_DEV_TDD_VLP_v33.docx	CALT
D68	doc52016	FDSH_RD_BSD_VLP_v33.docx	CALT
D69	doc54696	FDSH_DEV_TDD_EE.docx	CALT
D70	doc54694	FDSH_DEV_TDD_APC_T.docx	CALT
D71	doc54695	FDSH_DEV_TDD_AT.docx	CALT
D72	doc54698	FDSH_DEV_TDD_IFSV_T.docx	CALT
D73	doc54699	FDSH_DEV_TDD_MFA_UM_UA.docx	CALT
D74	doc54700	FDSH_DEV_TDD_RIDP_PI_FARS.docx	CALT
D75	doc54701	FDSH_DEV_TDD_SSA_Comp.docx	CALT
D76	doc54702	FDSH_DEV_TDD_VerCurInc_T.docx	CALT
D77	doc54703	FDSH_DEV_TDD_VerESIMEC.docx	CALT
D78	doc54704	FDSH_DEV_TDD_VLP_v32_1.docx	CALT
D79	doc54705	FDSH_DEV_TDD_VLP_v33.docx	CALT
D80	doc54706	FDSH_DEV_TDD_VerNonESIMEC.docx	CALT
D81	doc52021	FDSH_RD_BSD_Trading_Partner_Onboarding.docx	CALT
D82	doc42857	FDSH_RD_BSD_EDI_820_FEPS_Payment_Issuers_Service.docx	CALT
D83	doc42858	FDSH_RD_BSD_Enrollment_999_Reporting.docx	CALT
D84	doc42859	FDSH_RD_BSD_Exchange_Enrollment.docx	CALT
D85	doc42867	FDSH_RD_BSD_Verify_Non_ESI_MEC.docx	CALT
D86	doc42868	FDSH_RD_BSD_Verify_ESI_MEC.docx	CALT
D87	doc26944	TWS_FDSH_User Guide_v01.doc	CALT
D88	artf105388	MID Simulating the multi Thread for batch Processers not working as expected (Placeholder story)AS RRJ ETL Specification Document	CALT
D89	artf87043	Batch File Receiver Component	CALT
D90	doc15198	MIDAS_Implementation Plan V0.5	CALT
D91	artf87668	As the Hub, determine the structure of batch manifest documents	CALT
D92	artf95691	Batch orchestration	CALT
D93	artf93357	Batch Manifest Validator	CALT
D94	artf96015	Batch Orchestrator (Design)	CALT
D95	artf97293	Batch Orchestration: BOM Responder	CALT
D96	artf97295	Batch Orchestration: Batch Processor(s)	CALT
D97	artf97290	Batch Orchestration: BOM Listener	CALT
D98	artf97292	Batch Orchestration: Batch Orchestration Module (BOM)	CALT
D99	artf128420	Batch Framework refactor for IRS	CALT
D100	artf98131	MarkLogic Batch Process Module	CALT
D101	artf97342	Batch State Schema Definition	CALT
D102	artf87691	As the Hub, determine the strategy for processing of Batch Files	CALT
D103	artf87238	As the Hub, delegate a batch file to Application Zone for processing	CALT
D104	artf87237	As the Hub, delegate a batch file to MarkLogic for processing	CALT
D105	doc27080	FDSH_PROC_Development.docx	CALT

D106	N/A	FDSH Project/Dashboard	CALT
D107	N/A	Data Services Hub	CALT
D108	doc54465	R7Sprint20_Test Plan	CALT
D109	artf125921	PM issues with checksum and bulk DMSClient “FDSH.bulk.webService.save.location" location	CALT
D110	N/A	FDSH_Plan_Test, FDSH SOW, FEPS Test Plan, 5/24/12	GTL
D111	N/A	FEPS Testing Framework v6, v7, FEPSPerStratTest -Oct 10 v2, Federal Testing presentation 11/14/12	GTL
D112	N/A	FDSH Interview Notes-11/01/12	GTL
D113	doc54521	CM Readiness Review Checklist Sprint21 Release7	CALT
D114	doc49468	CM Readiness Review Checklist Sprint20 Release6	CALT
D115	doc5205	FFE Process Agreements DRAFT V1.xlsx	CALT
D116	doc10008	Local MarkLogic Setup Guide	CALT
D117	doc31409	FDSH_Planning_Schedule.mpp (as of October 1, 2013)	CALT
D118	doc43677	CDM Master Schedule.mpp (As of October 4, 2013 update)	CALT
D119	N/A	CCIIO Resource Allocations by Project - ECPE Cloud 20130517.pdf	GTL
D120	doc48809	FDSH_SEC_ISCP.docx	CALT
D121	doc29501	Secure Communications - Application Later Connectivity Test (SSA)	CALT
D122	doc45582	Secure Communications - Application Layer Connectivity Test (IRS)	CALT
D123	doc29440	Secure Communications - Application Layer Connectivity Test (Medicare)	CALT
D124	doc53568	FDSH_Plan_Configuration_Management	CALT
D125	N/A	FDSH Project Management Plan (PMP), Version 1.0, March 2012	GTL
D126	N/A	QSSI Karlton Kim on 11/18/2012	Interview
D127	N/A	FDSH Project Management Plan (PMP), Version 1.0, March 2012	GTL
D128	N/A	Interview conducted on July 12, 2012	Interview
D129	N/A	Project: Data Services Hub- Reports Tab- RTM- Reports Details- Filter by Release 3, Sprint 7, 8, and 9, HIX FDSH (Q3 – 2012) Release 3 (Sprint 9) IT Release Notes	CALT
D130	N/A	FDSH-Reports- RTM	CALT
D131	doc43174	FDSH_TST_FFEHUB_IntegrationProfiles_Sprint19V10_4	CALT
D132	doc31409	FDSH_Planning_Schedule.mpp (as of October 1, 2013)	CALT
D133	doc45955	pmTransferReport_2013810-100.255528.csv	CALT

APPENDIX D: RISK DETERMINATION

D.1 RISK DESCRIPTION

Findings identified in this assessment must be associated with several metrics factors to help determine the level of risk value related to a specific element or process. Risk is defined as the combination of the probability of occurrence and the consequences of a given future undesirable event. Risk can be associated with products and/or projects.

The determination of risk or vulnerability can be expressed as a function of:

- The likelihood (probability) of a given finding posing a risk to system development or functionality
- The magnitude of the impact of a finding posing a risk to system development or functionality

Where:

P = Probability
I = Impact
and: P x I = Risk Score

To measure risk, a risk scale and a risk-level matrix has been developed.

D.2 RISK DETERMINATION

Table D-1 displays the Risk Scale and required actions. This risk scale, with its ratings of High, Moderate, and Low, represents the degree or level of risk to which a system, facility, or procedure might be exposed to a given vulnerability were exercised. The risk scale also presents actions that senior management, the mission owners, must take for each risk level.

Table D-1 Risk Scale and Necessary Actions

Risk Rating	Action Implementation
High	High-risk levels create a strong need for corrective actions and the creation of an action plan that is put in place as quickly as possible.
Moderate	Moderate-risk levels warrant corrective actions and a plan to incorporate those actions within a reasonable period of time.
Low	For low-risk levels, the application owner must decide whether corrective actions are needed or whether the risks may be accepted.

D.3 RISK MITIGATION AND RECOMMENDATIONS

During the risk mitigation process, controls that could mitigate or eliminate the identified risks are provided. The goal of the recommended controls is to reduce the level of risk to FMPS and its data to an acceptable level.

The following factors should be considered in recommending controls and alternative solutions to minimize or eliminate identified risks:

- Effectiveness of recommended options (e.g., system compatibility)
- Organizational policy
- Operational impact

For consistency and clarity and to maintain an accurate understanding of risk findings, IV&V adopted the CMS risk management methodology, as defined in the Risk Management Plan (CMS RMP – '*CMS Health Insurance Exchange Risk Management Plan v 1.1_04302012_Draft'*); accordingly, risks identified on the FFM project level will be shared with partner and stakeholder groups for visibility and shared understanding of FMPS project risks to support successful risk management at the project level and through the enterprise level through correlation to the FFM Integrated Master Schedule (IMS) milestones and tasks. The intent is to identify and appropriately address and elevate project risks to the Health Insurance Exchange Program level for visibility, mitigation and for possible action.

Each risk is documented as fully as possible to include probability (likelihood), impact, risk value, system & scope assessment area and overall characteristic. As a part of the documentation of the risk, a nominal probability (likelihood) and impact rating on the risk finding was submitted and was mathematically factored to reach an overall risk value. See Tables 2-3, 2-4, and 2-5 for probability, impact and risk value guidance.

Table D-2 Probability Assessment Criteria

Level	Probability	Probability of Occurrence
5	Near Certainty	81-99%
4	Highly Likely	61-80%
3	Likely	41-60%
2	Low	21-40%
1	Not Likely	5-20%

Table D-3 Impact Assessment Criteria

Level	Impact
5	Severe degradation in technical threshold performance; jeopardizes project success. Cannot meet key milestones. Represented as a 20% deviation of the baselined plan.
4	Significant degradation in tech performance, unacceptably below goals, no design margins. Requires program or project critical path change. Represented as a 15–20% deviation of the baselined plan.
3	Moderate shortfall in tech performance, with limited impact; technical goals unmet and design margins significantly reduced. Schedule slip impacts milestone (MS) or Critical path slack. Represented as a 10–15% deviation of the baselined plan.
2	Minor reduction in technical performance, but can be tolerated, little impact; goals and design margins reduced. Schedule slip but will meet MS. Represented as a 5–10% deviation of the baselined plan.
1	Minimal consequence to performance, but no overall impact; goals and design margins will be met. No schedule slip. < 1% increase from baseline.

Table D-4 Risk Value

Risk Value Exposure Score	Risk Level
15-25	High
6-14	Moderate
1-5	Low

APPENDIX E: FMPS IV&V CODE REVIEW TOOLS

Table E-1 Code Review Tools

Tools	Source	Usage
Sonar - Toxicity Chart Plugin	http://docs.codehaus.org/display/SONAR/Toxicity+Chart+Plugin	Generate graphical views of key concerns across the entire code base.
Sonar - JavaScript Plugin	http://docs.codehaus.org/display/SONAR/JavaScript+Plugin	Analyze JavaScript files to identify potential compatibility issues or code defects. Using the Sonar plugin also provides a means to actively manage reviews of violations (unlike JSHint).
JHawk Java Metrics Tool	http://www.virtualmachinery.com/jhawkprod.htm	Generate tables of various metrics to compare to industry guidelines and identify potential problem areas.
JSHint/Rhino	https://github.com/jshint/jshint/ Download: http://www.jshint.com/platforms/ Download: https://developer.mozilla.org/en-US/docs/Rhino/Download_Rhino	Analyze JavaScript files to identify potential compatibility issues or code defects. Rhino is the Java-based JavaScript engine needed to run the JSHint library on other JavaScript modules. (Also used by CMS, but we cannot access the server that holds the JSHint results)
BeyondCompare	http://scootersoftware.com/	Compare Sonar Quality Profiles

APPENDIX F: DETAILED CODE REVIEW FDSH

Table F-1 Critical Violations Findings FDSH

Function	Project	Source	Date Evaluated
	FDSH	Java	10/29/2013
Package / Class	**Method**	**Findings**	**Used By Which Service**
gov.hhs.cms.hix.FDSH.ee.irs.actions	FileSenderIRSResponseAction	Dodgy - Dead store to local variableStmt	
gov.hhs.cms.hix.FDSH.ee.dhs.actions	PrepareRequestForSubmitAdditVerifAction	Dodgy - Dead store to local variableStmt	
gov.hhs.cms.hix.FDSH.ee.nonesi_mec.ext	ExternalNonEsiMecServiceImpl	Dodgy - Dead store to local variableStmt	
gov.hhs.cms.hix.FDSH.ee.ssa.ext	ExternalSSAServiceImpl	Dodgy - Dead store to local variableStmt	
gov.hhs.cms.hix.FDSH.ee.ridp	RIDPRESTClientAction	Dodgy - Write to static field from instance method	
gov.hhs.cms.hix.FDSH.ee.ffe.actions	FFEIRSErrorTranslationAction	Dodgy - Write to static field from instance method	
gov.hhs.cms.hix.FDSH.ee.esimec	DetermineESIEligibilityCodesAction	Dodgy - Write to static field from instance method	
gov.hhs.cms.hix.FDSH.ee.dhs.actions	GetNextResolvedCaseRequestAction	Dodgy - Write to static field from instance method	
gov.hhs.cms.hix.modules.ee.ruleset	IRSBulkRequestValidator	Correctness - Possible null pointer dereference	
gov.hhs.cms.hix.FDSH.common.dal	SyncDataServiceEvent	Correctness - Possible null pointer dereference	
gov.hhs.cms.hix.FDSH.core.actions.support	BatchTransferWindowCachingService	Correctness - Possible null pointer dereference	
gov.hhs.cms.hix.FDSH.core.actions.jms	JMSUtil	Correctness - Possible null pointer dereference	
gov.hhs.cms.hix.FDSH.ee.ridp	PrepareRIDPRequest	Performance - Inefficient use of keySet iterator instead of entrySet iterator	
gov.hhs.cms.hix.FDSH.ee.ridp	RIDPRESTClientAction	Correctness - Possible null pointer dereference	

gov.hhs.cms.hix.FDSH.ee.dhs.actions	GenerateDhsVerCasesRequestAction	Correctness - Possible null pointer dereference	
gov.hhs.cms.hix.FDSH.common.dal.converters.xcc	CaseWorkflowXccConverter	Correctness - Possible null pointer dereference	
gov.hhs.cms.hix.FDSH.common.dal.pojo	CaseResponse	Security - Array is stored directly	
gov.hhs.cms.hix.FDSH.ee.dhs.ext	SubmitThirdVerifResp	Security - Array is stored directly	
gov.hhs.cms.hix.FDSH.common.dal.pojo	DMSRequest	Security - Array is stored directly	
gov.hhs.cms.hix.FDSH.common.dal.pojo	FileRequest	Security - Array is stored directly	
gov.hhs.cms.FDSH.services.ee.vclp.wsdl	CertifyLawfulPresenceStep3SIB	Performance - Private method is never called	
gov.hhs.cms.hix.FDSH.ee.esimec	MockOPMQueryAction	Performance - Private method is never called	
gov.hhs.cms.hix.FDSH.common.esb.gw	XmlPayloadServiceInvoker	Performance - Private method is never called	
gov.hhs.cms.hix.modules.bulkFile.manifest	AttachmentFile	Bad practice - Method may fail to close stream on exception	
gov.hhs.cms.hix.FDSH.common.utils.io	FDSHFileUtils	Bad practice - Method may fail to close stream on exception	
gov.hhs.cms.hix.FDSH.ee.dhs.actions	VLPStep1FineAction	Correctness - Call to equals() comparing different types	
gov.hhs.cms.hix.FDSH.common.dal.converters.xcc	BatchXccConverter	Correctness - Call to equals() comparing different types	
gov.hhs.cms.hix.FDSH.bulkFile.esb.orchestration	BatchOrchestrationListener	Correctness - Nullcheck of value previously dereferenced	
gov.hhs.cms.hix.FDSH.ee.dhs.cases	CaseWorkflowManager	Correctness - Call to equals() comparing different types	
com.marklogic.ps.util	TimedHashMap	Correctness - An apparent infinite recursive loop	
gov.hhs.cms.hix.FDSH.core.actions.support	BatchTransferWindowCachingService	Correctness - An apparent infinite recursive loop	
com.marklogic.ps.util	PooledObjectIterator	Bad attempt to compute absolute value of signed 32-bit hashcode	
gov.hhs.cms.hix.FDSH.core.actions.jms	JMSUtil	Correctness - Unnecessary type check done using instanceof operator	

gov.hhs.cms.hix.FDSH.ee.plan.mgmt.actions	ManifestDocumentPojo	Bad practice - Class defines equals() and uses Object.hashCode()	
gov.hhs.cms.hix.FDSH.core.actions.jms	JMSUtil	Empty Finally Block	
gov.hhs.cms.hix.FDSH.common.utils.io	FDSHFileUtils	Empty While Stmt	
gov.hhs.cms.hix.FDSH.ee.dhs.ext	ExternalDHSServiceImpl	Dodgy - Method uses the same code for two branches	
gov.hhs.cms.hix.FDSH.ee.plan.mgmt.actions	ManifestDocumentPojo	Equals Hash Code	
gov.hhs.cms.hix.FDSH.dal.dao	SystemOfRecordDelegateImpl	Performance - Method uses toArray() with zero-length array argument	
gov.hhs.cms.hix.FDSH.core.actions.jms	JMSUtil	Bad practice - Class defines compareTo(...) and uses Object.equals()	
gov.hhs.cms.hix.FDSH.common.dal.converters.**xcc**	BatchXccResponseConverter	Empty If Stmt	

Table F-2 Major Violations Findings FDSH

Function	Project	Source	Date Evaluated
	FDSH	Java	10/29/2013
Package / Class	**Method**	**Findings**	**Used By Which Service**
gov.hhs.cms.hix.modules.bulkFile.web.util	BatchWSUtil	Avoid commented-out lines of code	
gov.hhs.cms.hix.FDSH.ee.irs.actions	FileSenderIRSResponseAction	Avoid commented-out lines of code	
gov.hhs.cms.hix.modules.ee.ruleset	CommonValidator	Avoid commented-out lines of code	
gov.hhs.cms.hix.FDSH.core.actions.pm	PartnerManagementDSLAction	Dodgy - Exception is caught when Exception is not thrown	
gov.hhs.cms.hix.FDSH.ee.currentincome.ext	ExternalCurrentIncomeServiceImpl	Dodgy - Exception is caught when Exception is not thrown	
gov.hhs.cms.hix.FDSH.core.actions.tp	TradingPartnerManagementDSLAction	Dodgy - Exception is caught when Exception is not thrown	

gov.hhs.cms.hix.FDSH.ee.actions	VerifyCurrentIncomeAction	Dodgy - Exception is caught when Exception is not thrown	
gov.hhs.cms.hix.FDSH.core.actions.jms	JMSUtil	Cyclomatic Complexity	
gov.hhs.cms.hix.FDSH.ee.dhs.actions	RetrieveCaseResolutionAction	Cyclomatic Complexity	
gov.hhs.cms.hix.FDSH.ee.dhs.actions	TranslateEligCodeAction	Cyclomatic Complexity	
gov.hhs.cms.hix.FDSH.ee.dhs.actions	CaseWorkFlowDALAction	Cyclomatic Complexity	
gov.hhs.cms.hix.FDSH.core.actions.pm	PartnerManagementDSLAction	Preserve Stack Trace	
gov.hhs.cms.hix.FDSH.core.actions.rc	RequestAssociationAction	Preserve Stack Trace	
gov.hhs.cms.hix.modules.bulkFile.manifest.builder	ManifestBuilder	Preserve Stack Trace	
gov.hhs.cms.hix.FDSH.core.actions.rc	RequestAssociationDSLAction	Preserve Stack Trace	
gov.hhs.cms.hix.FDSH.common.dal.pojo	BatchRequest	Visibility Modifier	
gov.hhs.cms.hix.FDSH.common.dal.pojo	CaseResponse	Visibility Modifier	
com.marklogic.ps.util	TimedHashMap	Visibility Modifier	
gov.hhs.cms.hix.FDSH.common.dal.pojo	DalResponse	Visibility Modifier	
gov.hhs.cms.hix.FDSH.core.actions.jms	JMSUtil	Signature Declare Throws Exception	
gov.hhs.cms.hix.FDSH.core.actions.jms	DynamicJMSRouterAction	Signature Declare Throws Exception	
gov.hhs.cms.hix.FDSH.bulkFile.esb.orchestration	MockBatchServiceAction	Signature Declare Throws Exception	
gov.hhs.cms.hix.FDSH.common.client	RESTClientAction	Reliance on default encoding	
gov.hhs.cms.hix.FDSH.core.actions	RESTXMLClientAction	Reliance on default encoding	
gov.hhs.cms.base.common.security.util	EncryptionUtil	Reliance on default encoding	

gov.hhs.cms.base.common.security.util	PasswordVault	Avoid Throwing Raw Exception Types	
gov.hhs.cms.hix.FDSH.core.actions.eip.sa.aggregation.store	AggregationStoreFactory	Avoid Throwing Raw Exception Types	
gov.hhs.cms.hix.FDSH.dms.dal.ejb	DMSFileRequestMDB	Avoid Throwing Raw Exception Types	
gov.hhs.cms.hix.FDSH.common.dal.pojo	CaseRequest	Loose coupling	
gov.hhs.cms.hix.FDSH.common.dal.pojo	CaseResponse	Loose coupling	
gov.hhs.cms.hix.FDSH.ee.dhs.actions	TranslateEligCodeUtil	Loose coupling	
gov.hhs.cms.hix.FDSH.ee.irs.actions	FileSenderIRSResponseAction	Unused local variable	
gov.hhs.cms.hix.FDSH.ee.irs.actions	PrepareRATIrsAction	Unused local variable	
gov.hhs.cms.hix.FDSH.ee.incarceration.ext	MockExternalIncarcerationStatusServiceImpl	Naming - Suspicious constant field name	
gov.hhs.cms.hix.FDSH.common.dal.converters.xcc	PartnerManagementRequestXccConverter	Performance - Unread field: should this field be static	
gov.hhs.cms.hix.FDSH.ee.non esi_mec.ext	ExternalNonEsiMecServiceImpl	Static Variable Name	
gov.hhs.cms.hix.FDSH.common.dal.pojo	CaseResponse	Malicious code vulnerability - May expose internal representation by returning reference to mutable object	
gov.hhs.cms.hix.modules.bulkFile.web.util.logging	BulkWebEventLogger	Non-transient non-serializable instance field in serializable class	
gov.hhs.cms.hix.FDSH.ee.esimec	ESIMECApplicant	Constructor Calls Overridable Method	
gov.hhs.cms.hix.FDSH.ee.esimec	ESIMECResponse	Constructor Calls Overridable Method	
gov.hhs.cms.hix.FDSH.ee.non esi_mec.ext	ExternalNonEsiMecServiceImpl	Performance - Unread field	
ffe.cms.hhs.gov	CaseDataType	Bad practice - Confusing method names	
gov.hhs.cms.hix.modules.bulkFile.manifest	EftManifest	Avoid cycle between java packages	
gov.hhs.cms.hix.FDSH.util	EMFUtil	Avoid cycle between java packages	

gov.hhs.cms.hix.FDSH.ee.dhs.actions	RetrieveCaseResolutionAction	Boolean Expression Complexity	
gov.hhs.cms.hix.modules.bulkFile.manifest.builder	ManifestPreValidator	Performance - Could be refactored into a named static inner class	
gov.hhs.cms.hix.FDSH.ee.currentincome.ext	ExternalCurrentIncomeServiceImpl	Big Integer Instantiation	
gov.hhs.cms.hix.FDSH.bulkFile.esb.orchestration	ESBBatchProcessor	Avoid Catching NPE	
gov.hhs.cms.FDSH.services.ee.vclp.wsdl	CertifyLawfulPresenceStep3SIB	Unused private method	
gov.hhs.cms.hix.FDSH.core.actions.jms	JMSUtil	Performance - Should be a static inner class	

Exhibit 11

Transcript of House Committee on Energy and Commerce. Subcommittee on Oversight and Investigations. Security of HealthCare.gov. Nov. 19, 2013. Testimony of Henry Chao. 302.

CQ CONGRESSIONAL TRANSCRIPTS
Congressional Hearings
Nov. 19, 2013 - Final

House Energy and Commerce Subcommittee on Oversight and Investigations Holds Hearing on HealthCare.gov Security

LIST OF PANEL MEMBERS AND WITNESSES

MURPHY:

Good morning. I convene this hearing of the Subcommittee on Oversight and Investigations to discuss the security of the healthcare.gov website. Americans want to know the answers to two simple questions. Is my information secure if I use healthcare.gov? And why should I believe the administration that it is?

It's been nearly 50 days since the launch of healthcare.gov and the website is still not functioning at an acceptable level. This is despite the numerous promises in assurances the public was given by members the administration leading up to and over the several months up to the launch of the website.

This Committee heard directly from Secretary Sebelius, Administrator Tavenner, and CCIIO director, Gary Cohen that they were ready by October 1. We're all deeply troubled that the individuals who want to be in charge of America's healthcare system could not even predict the accuracy (ph) of the website would work. And those predictions were not just limited to the website.

We've also been routinely promised that the website was safe and that Americans' personal information would be secure. When Administrator Tavenner last appeared before this Committee, she informed us that testing began on October of last year. But end in testing would be completed by the end of August this year. We have now learned that this simply was not the case. End to end testing is not possible when the website isn't completed.

Today we hope to hear form our witness about how much of the website remains to be built. If the first part of the healthcare.gov have been this problematic, we're obviously concerned about parts that have been constructed under current pressures and time constraints. The witnesses for -- the witness for our first panel today is Mr. Henry Chao, the Deputy Chief

Information Officer at the Centers for Medicare and Medicaid Services. And we want to thank you for coming and testifying today. We can only imagine how stressful the last few months have been for you. So welcome here.

Yet I hope you can appreciate the fact that HHS says ways to go to regain the trust of the American people on this website. And they were promised a functioning website as easy as buying a TV in Amazon and what they got was train wreck. The reason the trust of the American people maybe so difficult to regain is because everyday new revelations emerges show this wreck was entirely foreseeable. Last week this subcommittee uncovered e-mails CMS showing that as early July of this year, Mr. Chao, our first witness was worried that the company primary responsible for building the website, CGI would "crash the takeoff."

Today this subcommittee also released materials showing that as early as March to April of this year, top administration officials were well-aware that healthcare.gov was far-off schedule and testing of the website would be limited. We have also learned that healthcare.gov was only launched after Administrator Tavenner signed an authority to operate which included a memo warning her that a full security control assessment was not yet completed. This memo makes it clear that the highest levels of CMS knew that that there were security risks present. Yet again, while this document was being signed in private, administration officials were promising in public that in only a few days, the American people would be able to use a perfectly functioning website.

A few weeks ago Secretary Sebelius told this Committee that the highest security standards are in placed and people have every right to respect privacy. I hope that today we hear what those standards are from -- not only from Mr. Chao, and also from our second panel as well.

Our second panel features some of the contractors that are responsible for the security of healthcare.gov. And I thanked them for testifying today. I'm disappointed that one of the companies responsible for security, Verizon, chose not testify today. We will certainly be following with Verizon so that they are accountable to the public for their work here.

Today's hearing is not just about the website. Websites can be fixed, what cannot be fixed is the damage that could be done to the American people if their personal data is compromised. Right now, healthcare.gov screams to those who are trying to break into the system. If you like my healthcare info, maybe you can steal it. But I now recognize for an opening statement, Ms. Degette of Colorado for five minutes.

DEGETTE:

Thank you very much, Chairman Murphy. I want to add to your thanks to Mr. Chao for being here today, as well as the three contractor witnesses MITRE, CCSi and Foreground. We must make sure that the healthcare -- that the data on healthcare.gov is secure. Everybody can agree on that. The American people must know that their data is protected when they go on the site to find a quality, affordable insurance plan for themselves and their families.

This is critical. However my fear is that today's hearing is actually less about the facts that the security of healthcare.gov and more about political points and undermining the ACA. Now, without a doubt no one could disagree there are troubling problems with the rollout of the exchanges. Three weeks ago, our full Committee held the first hearing on the inexcusable fact that healthcare.gov seems to be have broken since its very first launch. And three weeks later while improving, it's clearly not up to speed. As I have said before, the exchanges need to be fixed and they need to be fixed fast so that the America people can easily access quality, affordable insurance plans open to them. I hope we'll have another hearing after the November 30th deadline to see how they are working.

My fear about this hearing today though is that it won't enlighten the American public but instead raise unjustified fears about security piling on all of the other issues. Now obviously as I said, we need to make sure that the data on healthcare.gov is secure, but we should not create smoke if there's no fire. So before we begin, I want to give the American people some peace of mind based on the facts that we know about security on healthcare.gov.

First and critically, no American has to provide any personal health information to healthcare.gov or to insurers in order to qualify for health coverage and subsidies. To make sure about this, I went on the Exchange myself the other day and that's because the ACA bans discrimination based on pre-existing health conditions. Before the ACA became law, Americans buying coverage on the individual insurance market had to fill out page after page of personal health information to apply for insurance. But no longer, thanks to Affordable Care Act, Americans do not have to turn over any private health insurance to get coverage.

Second, while no website in the government or in the private sector is 100 percent secure unfortunately, there is a complex and detailed set of roles that HHS must follow to make sure that data on healthcare.gov is secure. And I'm looking forward to hearing from you, Mr. Chao about these security issues today.

The agency has a long record of maintaining personal information about Medicare, Medicaid, Social Security and many areas and has never had significantly give information. HHS must comply with the Federal Information and Security Management Act and National Institute of Standards in Technology Guidelines to protect information systems and the data collected are maintained by healthcare.gov. And like all federal agencies, HHS is required to develop document and implement an agency-wide information security program.

To date, our Committee's investigation has found that CMS has complied with every important security rule and guideline. They hired a small army of contractors to make sure the website is secure. And they are going to talk to us about it today.

The memo, Mr. Chairman that you talked about in our last hearing, that identified some security concerns primarily a lack of end to end testing on healthcare.gov. But it also outlined the mitigation plan, one we learned was that the agency was following to mitigate security risk. So I want to hear from the contractors and from you, Mr. Chao, if in fact these findings are being heeded.

Now unfortunately, Mr. Chairman I have to raise one more issue in my remaining minute. And that is, this Committee's grand tradition of bipartisanship investigation. Apparently, the Committees, last Thursday, received a memo from CMS Red Team discussion document. The majority on this Committee did not hear this memo with the minority on this Committee, and so yesterday, coincidentally just after they leaked this memo to the Washington Post. Now -- and if you saw the Washington Post's front page today, you saw a big story, and Mr. Chairman, you were quoted in that story talking about concerns about the readiness of the exchange based on this memo.

I know that's not the topic of this hearing today. But I've got to say it is not in the tradition of the Committee to conduct investigations that way. And when the majority received this memo, it should have immediately provided it to all of the members so that we could read it and find out we are all just as concerned about making this exchanges work. And to that end, Mr. Waxman and I have written a letter expressing our displeasure. And we would like to enter that into the record at this time, Mr. Chairman.

MURPHY:

That's fine and I look forward to talk with you more about these procedures. I know that these came as part of hundreds of -- a couple of hundred thousand pages of documents were going through but we should -- well, I'm

glad to review that with you because I certainly respect my colleague on this ...

DEGETTE:
Certainly you were able to find it in time to give it to the Washington Post in time for today's hearing and to be quoted in the Washington Post.

MURPHY:
Well have a good discussion on that. I think, my colleague -- this time, (inaudible) I now recognize the Chairman of Full Committee, Mr. Upton for five minutes.

UPTON:
Well thank you, Mr. Chairman. You know, for months, the administration witnesses have come before this Committee and assured us that the implementation of the President's healthcare law was on track, their words. And that healthcare.gov would be ready for the October 1 launch. But why not give the straight story to the Congress and the public? Because back on April 18th, Secretary Sebelius testified in this very room, we have the Federal Hub on track and on time. I can tell you we are on track. Those are her words.

But we now know that the Secretary's testimony did not match what was happening behind the scenes. Two weeks before she testified before this Committee, Secretary Sebelius was present at an April 4th meeting where experts identified significant threats and risks launching the site on October 1st. The Administration was on track, on track for disaster. But stubbornly, they stayed the course, repeating their claims that this all was well and on track right up until the mess that launched on October 1. And even after they launched, the Administration officials insisted that the volume was primarily the culprit when they in fact knew otherwise.

But our oversight of the health law is not just about a website. No, it's not. It's about whether the public can trust in the law and this healthcare system that the Administration has been building for over three years and spending hundreds of millions of dollars. The failure of this website has significant consequences for all Americans. One important question is whether individuals will be able enroll and obtain coverage by January 1. Security is another critical concern. How can the public trust a hastily thrown together system in which meeting a deadline was more important for the Administration than conducting complete end to end testing of the sites security.

Mr. Henry Chao, Deputy Chief Information Officer of CMS is here to answer those questions about CMS's management of the federal exchange and the amplifications for security. Mr. Chao, I do understand that you're a career employee and had been at CMS for years. And I know, as Chairman Murphy indicated, the last few months have not been particularly easy.

Last March, you were one of the first to publicly offer a glimpse of the true situation when you candidly remarked about the website and said , "Let's just make sure its not a third world experience." Documents produced to the Committee paint a clear picture that the Administration officials in fact knew for months before the October 1 about the date about delays and problems with the website development. Mr. Chao, you have been responsible for managing the development of the healthcare.gov. But I could imagine many matters were outside of your control.

And given the lack of end to end testing, I hope that you can explain to us today why the Administration felt confident in the security of healthcare.gov when the system went live on October 1. We're also joined by three companies that were awarded contracts by CMS to provide security services for the federal exchange. These companies are here also today to answer questions about their roles. And I know the subject of security presents certain sensitivities. And I'm glad that they made the decision to accept our invitation to testify and inform us about how healthcare.gov works or doesn't.

One thing that we have learned, there are countless contractors involved in building this website and responsibilities are divided, very divided. It is a complex system I know, but we'd like to know how the delays and rush of implementation have affected or complicated the ability to perform the security work for the website. And I yield the balance of my time to Dr. Burgess.

BURGESS:
I thank the Chairman for the recognition and I do want thank our witnesses for being here today. Pretty broad agreement to implementation of the Affordable Care Act has been problematic. And rather than getting better, it may be given worse. We got low enrollment numbers and websites so bad that it's required the appointment of glitch so far (ph), canceled plans, broken promises from the President just for starters.

These initial problems break surface of the deeper issues that lie ahead for not just to law but for the American people that must live under the law. And Mr. Chao, you probably -- prior to anyone else sounded the alarm of that speech they have. And I know you're tired of hearing it, but I will tell you once again, your comments that you're just trying to prevent the website

from becoming a third world experience. I admire your ability to see over the horizon and tell the problems before they come up and hit you in the windshield, but also you're the one who recommended that it was safe to launch the website on October 1st.

So, what happened in real six months that lead to yourself and others in the administration to believe that this law was in fact ready prime time. Not only did the Center for Medicare Medicate Services fail to establish basic functionality, but healthcare.gov's flaws continue to post a treat to the security of American's personal data. And just on a personal note, when I went to healthcare.gov this morning, it was still not functional, another website healthshper.com can actually tell me about the plans that are available in my area. We know it was possible to do this, we are all wondering why it wasn't? Thank you, Mr. Chairman, I yield back.

MURPHY:
... yields back, I now recognize the ranking members of the Full Committee, Mr. Waxman for five minutes.

WAXMAN:
Thank you very much, Mr. Chairman. The last six weeks has been a difficult one for supporter of the Affordable Care Act. The trouble rolled out of the website prevented many of our constituents who were signing up for the affordable, high quality coverage for which they now qualify. And it has been relentlessly exploited for political game by Republic opponents of the law. I was interested to hear the phrase in the two Republican statements, maybe and all of them. We don't want to third world website. But let me tell you what is third world. Third world in this country is when we live millions of people unable to get insurance because they have preexisting medical conditions, or they can afford it. No other industrial country allows such a thing to happen. But that what's the Republicans who have opposed this law would have us return to.

I think that we're turning the corner on the website on Friday, just (inaudible) to Administration's point person on heathcare.gov announced two key metrics of the improvement. And it seems to be this are all very good signs the website is getting better. Additional improvements are still needed but healthcare.gov means more and more people will me signing up the coverage as that website become more usable. I'll like to tell you what's happening in California, in the first month 35,000 people enrolled in the

exchange, over 70,000 qualified through Medicate and state officials say that the pace of enrollment is increasing. In just the first 12 days of November, enrollment from the first month almost doubled.

Now, I know we're looking today at the issue of data the security on healthcare.gov, it's an important issue. We should begin by engorging at the ACA represented an enormous step-forward for privacy because when people apply for insurance coverage, the law bends them for being asked questions about their underwriting, about their medical condition, about the privacy of things that affect their health. Because it's not necessary to ask those questions, they're not going to be denied insurance coverage because of previous medical problems.

But there are some personal information that people are going to be asked for when they sign up and they need to ensure that this information is protected. This question comes up repeatedly -- came up repeatedly to Secretary Sebelius (inaudible). She told us the development is placing a high priority on the security of the website and the higher security standards are in place to protect personal information on healthcare.gov.

I hope this hearing will be serious even-handed inquiry, but I fear that some of my Republican colleagues may exaggerate security concerns. The (inaudible) public fear and exaggerate it so that they could dissuade people from even signing up. This is exactly what this Subcommittee did when they launched an investigation into nonprofit community organizations serving as healthcare navigators.

They were harassing these people in order to prevent them from helping people, learn what's available to them. Mr. Chairman, yesterday we learn that you have been withholding important investigator documents, leaking them to the press before even providing them to the Democratic members and staff.

And I sent you a letter this morning describing why this is a violation of the Committee's president. It is not the way this Committee has traditionally operated and it raises concerns about whether these hearings are becoming another partisan attempt to weaken the Affordable Care Act.

The Committee should not go down that road. We should be using our oversight powers to improve the Affordable Care Act, not to sabotage it or to discourage Americans from signing up a quality care. I want to yield the balance of my time Mr. Chairman to Mr. Dingell.

DINGELL:

I thank the gentlemen. I ask you then Mr. Senator (inaudible) my remarks. I'm pleased to be here and I'm certainly pleased that my subscription for the Washington post is in effect so I can find out what's being leaked by my Republican colleagues to the media.

This is interesting. We have clearly a violation of the practices, traditions in history of this Committee and the investigations it's done. I speak as a member who's done more investigations than anybody in this room, including probably more than all of them put together. Here we have a beach of the responsibility of the leadership to make information available to the Committee at the same time they make it to the press. I find that difficult.

But worst than that, I find as intolerable that this Committee is running around fishing for trouble who are non-exist. I feel a little bit like the old maid who came home and look under the bed to find out if there is somebody there. Hoping in fact that there would be. Unfortunately, there is not.

I have seen no evidence of any complaints or any evidence of misbehavior with regards with the informations that is controlled by the government. I would urge this Committee to spend this time trying to make this situation work and see to it that we collect the information that's necessary, make the website work and see to it that we register the American so that we can cease being a third world nation, both with regard to how the Congress runs and how the healthcare of this country works.

We are down around this third world nations in the way that we take care of the health of our people. Look at this...

MURPHY:
Thank you, (inaudible).

DINGELL:
... it will give you a shock.

(UNKNOWN)
Gentleman's time has expired. Thank you very much.

And now I would like to introduce the witness on our first panel for today's hearing. Henry Chao has served since January 2011 as the Deputy Chief Information Officer and Deputy Director of the Office of Information Services at the Centers for Medicare and Medicaid Services. Some of his prior roles include Chief Information Officer in the Office of Consumer Information and Insurance Oversight and Chief Technology Officer for CMS.

And I'll swear in the witness, you are aware Mr. Chao that Committee has hold investigative hearing, and when doing so, has the practice of taking testimony under oath. Do you have any objections of taking testimony under oath?

Witness indicates no. The Chair then advises you that under the rules of the House and the rules of the Committee, you are entitled to be advised by council. Do you desire to be advised by council during your testimony today? Which your council indicates no. In that case, could you please rise, raise your right hand that swear you in.

Do you swear the testimony you are about to give, the truth, the whole truth and nothing but the truth? Thank you.

You're now under oath and subject to the penalty set forth in Title 18 Section 1001 of United States code. You may now give a five- minute summary of your written statement and make sure the microphone in on and pulled close to you. Thank you, Mr. Chairman.

CHAO:
Thank you, Chairman Murphy, Ranking Member Degette and members of the Subcommittee for inviting me to testify about the security of the federally-facilitated marketplace.

The security and protection of personal and financial information is a top priority for CMS, which for decades has protected the personal information of the more than 100 million Americans enrolled in Medicare, Medicaid and the Children's Health Insurance Program.

Protection of personal information in CMS program is a monumental responsibility. Everyday, CMS enrolls new Medicare beneficiaries, pays claims timely and efficiently, and protects the information of consumers and providers. CMS used this experience in our security best practices to build a secure federal marketplace that consumers should be feel confident entrusting with their personal information.

CMS follows federal law, government-wide security processes and standard business practices to ensure stringent security and privacy protection. CMS's security protections are not singular in nature, rather the marketplace is protected by an expensive set of security layers.

First and foremost, the application, the online application is developed with secure code. Second, the application infrastructure is physically and logically protected by our hosting provider. Third, the application is protected through an (inaudible) defense shield in order to protect

unauthorized access to any personal data. Finally, several entities provide direct and indirect security monitoring, security testing and security oversight which includes the various organizational groups that CMS are reporting to key stakeholders with respect to security and privacy.

This includes the Department of Health and Human Services. We also work in conjunction with U.S. CERT which is operated by Department of Homeland Security, CERT stands for Computer Emergency Response Team, and the Office of the Inspected General of HHS. Each of these groups have varying roles to ensure operational management and technical controls are implemented and successfully working.

The federally-facilitated marketplace is protected by the high standards, demanded of thorough information systems including regulations in the standards prescribed by FISMA, NIST, the Privacy Act and directed as promulgated by the Office of Management and Budget.

CMS designed the marketplace IT systems in the hub to reduce possible vulnerabilities and increase efficiency. A large number of connections can cause security vulnerabilities. The hub allows a one highly secured connection between highly protected databases of trusted states and federal agencies instead of hundreds of connections that would have been established as part of how normal business practices in present day, you know, how government connects organizations with each other to conduct business.

A series of business agreements enforce privacy and controls between CMS and our federal and state partners. Additionally, CMS designed the marketplace systems to limit the amount of personal data stored and protects personal information and limit access to passwords, encryption technologies, zoned architecture with Firewall separation in between the zones, and various other security controls to monitor logging and to prevent unauthorized access to our systems.

CMS also protects the federal marketplace, do intensive and stringent security testing. While the federal marketplace has had some performance issues that could have been addressed through more comprehensive functionality and performance testing, I want to be clear that we have conducted extensive security testing for the systems that went live on October 1st. We continue to test for security on a daily and a weekly basis any new functions or code prior to its launch. Of course we are working around the clock to fix our performance issues so that the vast majority of users have a smooth experience with the site by the end of the month.

Well, I cannot go into specific as far as security testing due to sensitive nature. I assure you that CMS conducts continuous anti- virus and malware scans, as well as monitors data flow and protections against threats by denying access to known source bad IP addresses and actors.

Additionally, we conduct two separate types of penetration testing on a weekly basis. The most recent penetration testing showed no significant findings. Also on weekly basis, CMS reviews the operation system, the infrastructure and the application software to be sure that these systems are compliant and do not have vulnerabilities. Vulnerabilities are often fixed immediately on site and retested to ensure the strength of our system's security. Each month, we review our plan of action and milestones in order to continuously improve our system security.

For the federally-facilitated marketplace, we conduct security control assessments on a quarterly basis, which is beyond the FISMA requirements. As of today, no vulnerabilities identified by our test have been exploited to (inaudible) attack.

Because of CMS's experience running trusted secure programs, our fulfillment of federal security standards and constant and routine security monitoring and testing, the American people can be confident in the privacy and security of the marketplace. Thank you and I'll be happy to answer your questions.

MURPHY:
Thank you, Mr. Chao. I'll recognize myself first for five minutes. Mr. Chao, for the last year, members of this Committee have asked you another -- and administration, about the status of the launch to the present healthcare law, we wanted to know if you would be ready of the October 1st start of enrollment.

Over and over, we were assured that all is well and everything was on track. The documents produced by the Committee show a different picture and I'd like to walk through a couple them with you.

In mid March, you made a candid comment that you didn't want the exchange website to be a third world experience. Now, the Committee has learned about a report prepared by Committee for Senior HHS and White House officials and presented to these officials in late March and early April this year, that document is tab one of your document binder. This document highlights a number of risks facing healthcare.gov's launch, late policy, delayed designs and building time and limited to a test. When did you first see this presentation?

CHAO:
I haven't seen that presentation.

MURPHY:
You were not briefed at all if there was a McKinsey report of presentation going on?

CHAO:
I knew that McKinsey had been brought in to conduct some interviews and assessments and report to our administrator in which I actually participated in some of those...

MURPHY:
You participated in the interviews when McKinsey was (inaudible)?

CHAO:
But I was not given the final report.

MURPHY:
We're you aware that they had met with Secretary Sebelius, Marilyn Tavenner, Gary Cohen and others at CMS headquarters, HSS headquarters, the Executive Office Building in the White House? Are any of those incidences?

CHAO:
I believe there were some meetings that I heard of, but I don't know that exact dates, you know, when they occured.

MURPHY:
Now part of your job is to make sure that this website is working, am I correct?

CHAO:
Correct.

MURPHY:

And so, this was a major report that went as high up as a sector maybe others we don't know. But saying that there were serious problems with this and you're saying that even though you were interviewed by this, you did not ever have this briefing yourself?

CHAO:
No, I didn't.

MURPHY:
You knew it existed?

CHAO:
I had heard that there was a final report out, but I didn't see the actual...

MURPHY:
Did anything change for you in recognizing this report or was that this briefing was out there basically telling people working on the HSS website that there were serious problems, no end to end testing at this -- all the area (inaudible)?

CHAO:
I can't really tell you or speak to the contents of that report because I did not see it and I didn't hear about it until actually it was in the Washington Post.

MURPHY:
And certainly, this is part of the concerns we have and we're not making this stuff up. It's a matter that we have a website out there which untold millions -- tens of million or hundreds of millions were spent on this website, which you have major leadership role here. McKinsey is hired to come and to present what the problems are and they had a roadmap with those problems.

I'm deeply concerned that this is something that you knew existed but have not read. So, when were you first concerned that the administration wasn't going to be ready October 1 for the start of the open enrollment?

CHAO:
I never though that. I've had...

MURPHY:

But you made a comment about you didn't want to see a plane crash.

CHAO:
Well, you're referring to the e-mail...

MURPHY:
Yes.

CHAO:
... exchange that I had with several...

MURPHY:
Yes, certainly, that e-mail didn't say, "Everything is going to fine, congratulations team."

(CROSSTALK)

MURPHY:
So you must have had some awareness that some problems existed.

CHAO:
Chairman, you have to understand and the Committee that I've been working on this since mid 2010.

MURPHY:
And we appreciate that.

CHAO:
And I've -- I'm a very cautious and, you know, I err on the side of caution and urgency because even back in 2010 I didn't believe that, you know, everything would be easy and just, you know, going along smoothly. So, on a regular basis, I work with a lot of my contractors and my staff to sensitize them on the sense and level of urgency that...

MURPHY:
Especially, McKinsey was called in to prepare this document which was important enough for them to have meetings at CMS, HSS with the secretary of Health and Human Services at executive office building and at the White

House, describing a level of problem. So, I appreciate your sensitivity and awareness to that, I'm concern you're saying you have not even read this yet.

Your testimony mentions the use of centers and active event monitoring, you state that if an event occurs, an instant response capability is activated, has that happened yet?

CHAO:
Yes.

MURPHY:
How many times?

CHAO:
You mean whether if we are conducting an...

MURPHY:
No, an instant response capability, or first of all, has anything happen yet, any hackers, any breaches, anyone trying to get into the system from the outside, has that occurred yet?

CHAO:
I think that there was one incident that I am aware of, but it requires that we go to a classified facility and (inaudible)...

MURPHY:
Only once since the -- you're saying no other attempts to breach into the system have occurred?

CHAO:
Not successful ones, no.

MURPHY:
Not, since when?

CHAO:
Not successful ones.

MURPHY:
All right. Now, when there are attempts, who do you report this to?

CHAO:
It's a combination of series of authorities that are involved, the law enforcement. Well, through our incident reporting and breach reporting processes that go through our agencies, a various key leadership, and then up through the department, as well we have a security incident response center at this department that works with U.S. CERT at DHS.

MURPHY:
Thank you. We'll follow up the Subcommittee. I have no amount time, so I will not recognize Ms. Degette for five minutes.

DEGETTE:
Thank you very, Mr. Chairman. First of all Mr. Chao and also to the contractors, something you said in your opening, I think we should really take heed which is you want to be careful not to divulge sensitive information about the security designs of the website, is that right?

CHAO:
That's correct.

DEGETTE:
So, I would say to you and to the contractors and I think that majority would agree with me, if there is a question asked about that sensitive information, if you would just let us know and then we can take into executive session or whatever we need to do.

CHAO:
Absolutely. Sure.

DEGETTE:
Thank you, Mr. Chairman. Now, Mr. Chao, the Chairman was asking you about this memo that you had or the e-mail and that was on Tuesday, July 16th, if you can take a look at tab seven in your binder, your document

binder please, that's a copy of your memo and it looks to me in reading it that you were basically telling people that you wanted to make sure this website got up and going, is that right?

CHAO:
Yes.

DEGETTE:
And that was your view, right?

CHAO:
Yes.

DEGETTE:
Did you take further actions after July 16th to try to get the website up and going.

CHAO:
It was a constant daily effort.

DEGETTE:
And it still is, isn't it?

CHAO:
To improve it, certainly.

DEGETTE:
Yes. OK. I'd like you now to take a look at tab one of your document binder. Now, Mr. Chao, this is the document that was given to the Washington Post yesterday by the majority and also simultaneously to the Democrats on the Committee. This was the document the Chairman was asking you about in his opening statement. Have you ever seen this document before?

CHAO:
No, I haven't.

DEGETTE:

OK. So, you don't really know about whatever it might have said in that document, right?

CHAO:
No.

DEGETTE:
OK. Thanks.

CHAO:
I believe it's an executive level briefing for...

DEGETTE:
Right. But you'd work -- you didn't -- you were part of that briefing?

CHAO:
No.

DEGETTE:
OK. That doesn't mean through that you weren't concerned about the website working in time to make it work.

CHAO:
Of course. I think in some of the interviews with McKinsey, you know, I think some of what's in here could have potentially come from information that...

DEGETTE:
But you wouldn't know that because you didn't see.

CHAO:
No, I'd see....

DEGETTE:
I want to talk to you about the topic of this hearing now for a few minutes, and that is the issue of security. And I think I heard you say both in your opening and response to questioning by the Chairman, I just wanted to ask

you again, have there been vulnerabilities that have been discovered since the website (inaudible) on October 1st?

CHAO:
Security vulnerabilities...

DEGETTE:
Yes.

CHAO:
... have not necessarily been reported in terms of it being a security threat. I think there were some misuse of terminology of something like 16 incidents reported that in a previous DHS testimony a couple of days ago. But they were actually incidents involving disclosure of PII information and it wasn't due to the result of anyone trying to attack the website.

DEGETTE:
What was said (ph) the result of?

CHAO:
It was dealing with some training issues at the call center or we had a system issue where you if you had similar usernames we had -- and you chose a special character at the end of that username. For example, if you -- your name is Smith and you chose an add sign at the end of the username, sometimes that add sign was treated like a what we call a wild card search so they'll return a log-in information about someone else, but that since was reported has been fixed as of...

DEGETTE:
That problem had been fixed so that's not happening anymore.

CHAO:
It's not a hacker (ph)...

DEGETTE:
Now, you've been at the agency how long, sir?

CHAO:

Approximately 20 years.

DEGETTE:
And in working on the other sensitive areas Medicare and other areas, is this common that sometime there might be a little bump like this?

CHAO:
Fairly common.

DEGETTE:
And what does the agency do when that is identified?

CHAO:
We have an extensive set of processes and controls in place with a designated personnel to handle whether if there, for example, security breaches verus the -- personally-identifiable information type incidents, daily (ph) loss...

DEGETTE:
And there is continuing testing, is that right?

CHAO:
Correct.

DEGETTE:
Now, MITRE has been performing assessments for CMS, is that correct?

CHAO:
Correct.

DEGETTE:
And what that does is it gives the contractors the opportunity to identify and resolve security vulnerabilities, is that correct?

CHAO:

I think what's the benefit is that we use a set of contractors to independently test the system so that we're not picking the words of let's say for example QSSI or CGI themselves performing security testing. So this independent testing provides us a more, you know, balance view of...

DEGETTE:
And, is this on going, this...

CHAO:
Yes.

DEGETTE:
... this independent testing?

CHAO:
On a daily and weekly basis.

DEGETTE:
Thank you very much, Mr. Chairman.

MURPHY:
The Chair now recognize Mr. Barton for five minutes.

BARTON:
Thank you. Thank you, Mr. Chairman.

Hearing Mr. Dingell's opening statement and to some extent on what Ms. Degette just said, I'm reminded of the movie "Casablanca" and Claude Rains the French Chief of Police because in the Rick's Cafe and say's, "I'm shutting it down, I'm shutting it down." And Rick comes up who's played by Humphrey Bogart and says, "Why are you shutting us down?" And Claude Rains, the Chief of Police, says, "I'm shocked, shocked to learn there is gambling going on." Just as the creepy air comes up and says to Claude Rains, "You're winning, sir."

It is interesting and amusing that the past master are running this Committee, Mr. Dingell, would be shocked, shocked and amazed that something was given to the Washington Post yesterday. Now I'm not saying

that it was, I don't know, but if it did happen it wouldn't be the first time in this Committee's history that documents were given to the press at approximately the same time they were distributed...

DINGELL:
If the gentleman (inaudible) I didn't say I was shocked, I said I was grateful I had the subscription to the Washington Post so I could keep track what's going on the Committee (inaudible)...

BARTON:
Reclaiming my time for my -- which is my time from my good friend, what shocks me is that Mr. Chao, our witness, who is the Deputy Chief Information Officer and Deputy Director of the Office of Information and Services for Medicare and Medicaid who has been identified numerous times as the Chief Person in charge of preparing this website at the CMS level didn't -- was not aware of this document.

I mean, to me, that's what's shocking. So, my first question to you sir is, when were you made aware of this McKinsey briefing document?

CHAO:
I think I was aware that some document was being prepared because I had gone through the interviews, but towards the end when the briefings occurred, I was not a part of them, nor that was I...

BARTON:
Were you aware that McKinsey had been hired to come in and basically troubleshoot the status of the website?

CHAO:
I don't think they brought him to troubleshoot. I think they brought him to make an assessment by conducting various interviews with key stakeholders.

BARTON:
Did this group ever talked to you?

CHAO:
Yes

BARTON:
OK, so they did come in and at least visit with you?

CHAO:
Yes, they've interview me before

BARTON:
Once, twice, a dozen?

CHAO:
Well, probably at least two times from what I recall.

BARTON:
OK. Now, since you've been made aware of the document...

CHAO:
No, I...

BARTON:
... have you (inaudible) it?

CHAO:
No, I was not made aware of the document. I was interviewed by the team that put that together. When the document was assembled I didn't get a copy

BARTON:
OK, well, as Mr. Dingell has pointed out, it's in the Washington Post. So, have you - before coming before this Subcommittee this morning, have you perused this document?

CHAO:
No, I have not

BARTON:
You have not perused this document. OK.

Well, on page one of the document, it says, "The working group -- " whoever that is, maybe you can enlighten us on that -- "determine that extending the go live date" -- which as we all know is October the first -- "should not be a part of the analysis and therefore work with a boundary condition of October the 1st as the launch date." Now in plain English, what that means is, somebody decided we couldn't delay the start up date so (inaudible) we're going to assume it's going to go live on October the 1st. Were you a part of the working group that made that decision?

CHAO:
No.

BARTON:
Do you know who the working group was that made that decision?

CHAO:
No

BARTON:
Do you have any idea, was it the president and the secretary of Health and Human Services, or was somebody below your level that made a decision somewhere in the in the bowels of the bureaucracy?

CHAO:
I think that it probably was conglomerate of several conditions that came to that conclusion (inaudible).

BARTON:
Did you have any decision making authority yourself about when start up date should be?

CHAO:
No

BARTON:
That was not in your authority to say, "We're going to have to put it all" or make a decision to go forward?

CHAO:
No, I do not get to pick what date.

BARTON:
Do you know who did have that decision making authority?

CHAO:
I believe it's our Administrator, Marilyn Tavenner, and potentially other folks. But primarily, I take my direction from Marilyn Tavenner.

BARTON:
All right. Well, Mr. Chairman, my time is expired, but I'll just say in summing up, we're concerned at multiple levels, but if you review this CMS document which I did not see until just now, this morning, it does (inaudible) about 10 minutes ago to then look at it and it is absolutely clear that this - the start up of the website was not going work well if at all on October the 1st, it was not. And that it says that in here (ph). So with that, I yield back.

MURPHY:
Thank you. Gentleman's time has expired. The Chair now recognizes Mr. Dingell for five minutes.

DINGELL:
(Inaudible) for the recognition. I thank him for holding this hearing. We are over six months now and six weeks in the implementation of the Affordable Care Act. And while the personality of the healthcare.gov website has improved, it is clear there's more work to be done and I'm hopeful the Subcommittee will work hard to achieve that goal.

ACA is the law of the land and I believe we share the goal of making it a functioning and secure website. However, it's important to remember that we can never fully eliminate the risks when building a large IT system. And solely (ph) must take steps to mitigate them.

I'm going to also urge that we take the necessary steps to make the program work because this is the largest undertaking in this character. I believe that we have ever seen (inaudible) government anywhere.

First question, yes or no, is CMS responsible for developing the data services hub and the eligibility enrollment tools for the federally-facilitated marketplace? Yes or no, Mr. Chao.

CHAO:
Yes.

DINGELL:
Now, Mr. Chao, are these projects required to comply with the Privacy Act of 1974, the Computer Security Act of 1987, the Federal Information Security Management Act of 2002? Yes or no.

CHAO:
Yes.

DINGELL:
Now, additionally, CMS must also comply with regulations and standards promulgated by the National Institute of Standards and Technology at the U.S. Department of Commerce, is that correct?

CHAO:
Yes.

DINGELL:
Now, these NIST standards require CMS to balance security considerations with operational requirements, is that correct?

CHAO:
Yes.

DINGELL:
Mr. Chao, was the key pieces of healthcare.gov website is the data hub, is this a large repository of personal information as some of my friends on the other side have claimed? Yes or no.

CHAO:
No.

DINGELL:
Say that again, no?

CHAO:
No, it does not...

DINGELL:
OK, I want that on the record. We clearly heard. Does the data hub retain any personal information at all? Yes or no.

CHAO:
No.

DINGELL:
Indeed, is it fair to say that the data hub is a tool to transmit eligibility information to federal agencies? Yes or no.

CHAO:
Yes.

DINGELL:
Now, did the hub -- did the data hub pass a security test to the October 1 launch of healthcare.gov? Yes or no.

CHAO:
Yes.

DINGELL:
Is the data hub working as intended today? Yes or no.

CHAO:
Yes.

DINGELL:
Is there any evidence to the contrary?

CHAO:
No.

DINGELL:
Is there any evidence of breaches or lack of security of personal data or information by any person who has submitted such data to this undertaking? Yes or no.

CHAO:
No.

DINGELL:
It is always our duty to remember how our healthcare system operated (inaudible) the passage of the ACA. At that time, insurance companies were allowed to medically underwrite people to determine their premium. This required lengthy confusing applications and contain a lot of personal medical information, often times, this was submitted electronically as well. ACA has changed all of this.

Now, in fact, this is a question to you again, Mr. Chao -- in fact, application forms on healthcare.gov do not require the submission of any personal health information, is that correct? Yes or no.

CHAO:
Yes.

DINGELL:
Now, Mr. Chao, that's because ACA prohibits discrimination on the basis of preexisting conditions and outlaws charging people more because they are sick, is that correct?

CHAO:
Yes.

DINGELL:
So the information is not necessary?

CHAO:
No.

DINGELL:

Is that correct? It is not collected?

CHAO:
It's not collected.

DINGELL:
All right. This is a remarkable improvement over the older system in terms of both security and the quality of care. Next question, there are a lot of negative stories on the press that created a lot of confusion, so I want to get this record straight, is healthcare.gov safe and secure for my constituents to use today with regards to protection of their personal information and their privacy? Yes or no.

CHAO:
Yes.

DINGELL:
Is there any evidence at all to the contrary?

CHAO:
No.

DINGELL:
So, Mr. Chairman, you have been most precious, so I yield you back 12 seconds.

MURPHY:
Thank you. Now I'm going to recognize Ms. Blackburn. Thank you.

BLACKBURN:
And thank you, Mr. Chairman.

Mr. Chao, we really appreciate that you would come and work with us on this issue. I want to talk with you for a minute about some red flags that seemed to be apparent to you and you're going to find the e-mail I'm referencing at tab seven and it is the July 16th, 2013 e- mail that you sent to Monique Outerbridge. And I really want to focus there. You know, when you have something that is running off the rails and this obviously seemed to you to be doing, it was a project that just was not proceeding as it should be

proceeding, and you express these concerns about the performance of CGI. What I'd like to hear from you is just an articulation of maybe what were those top three of four red flags that seemed to be going up to you that you said, "I fear that the plane is going to crash on and take off" and some of those wordings that we have heard from you now, so give me just kind of the top three or four things.

CHAO:
I think in the context of this e-mail, it was at a time period in which we were getting ready to rollout what we called live account which is our initial registration process. And as I mentioned before, I'm a person who has a lot of anxiety and I err on the side of caution if we're going to run out time so I occasionally get a little passionate in my e-mails to remind people that they need to move fast. And if they are moving fast, they need to move faster. That's just the way I operate and the way I direct staff and cofactors. And what I was afraid of was at (inaudible) point in time was that we were falling behind the rollout of Live Account.

BLACKBURN:
OK. On live account did your test on that go of without a hitch, or what happened?

CHAO:
I don't exactly remember the specifics about web test passed or failed. I just was afraid that we were in jeopardy of missing the date, so therefore, you know, at that time period starting July wrote lots of e-mails to try to...

BLACKBURN:
Kicking (ph) up to date?

CHAO:
I believe we -- it took actually four days.

BLACKBURN:
An extra four days...

CHAO:
Yes.

BLACKBURN:
... on the test, and you don't remember exactly what the concerns were that came to you at that point of time? Is there a memo of review, a memo and an articulation of what transpired in that test process?

CHAO:
I don't think it's necessarily a memo. I think the way we operate is that we -- we have daily meetings...

BLACKBURN:
Are their minutes from those meetings and could you submit those to us for the record?

CHAO:
I don't believe that they were minutes. I believe they were just status check-ins, you know, contractors and their...

BLACKBURN:
Are there notes, informal notes?

CHAO:
I don't believe. So, I think when my e-mail were submitted as evidence...

BLACKBURN:
OK.

CHAO:
... that's kind of a...

BLACKBURN:
All right. Let me go on a minute. I want to talk specifically about CGI. What about -- you know, if you all kind of informally worked in a group and didn't have formal meetings or minutes and memos and things of that nature, just give me your impression. What was it your perception that caused you to lose confidence in CGI for where you on that? Because I think it's so interesting you mentioned price and I note in this e-mail chain from Monique Outerbridge that they had 40 million already that's (inaudible) taken, they

were coming back and asking for another 38 million. Now, if I had someone who had used the (inaudible) of their money from a project and then they came back and ask for that much more, I think I would have to say, "Wait a minute." So, regardless obviously the price to you was of tremendous concern, am I right on that?

CHAO:
Correct.

BLACKBURN:
OK. So they had already -- it kind of lose your confidence there, what else was it in their conduct that eroded your confidence in their ability to trans (ph) at this portion of business?

CHAO:
I think what I was trying to say is that relatively speaking to I would say most project managers they are looking at smaller scale projects. I would say there might be some room to be...

BLACKBURN:
OK.

CHAO:
... a little more confident but given what was the task at hand, my confidence level had to deal with the enormous amount of activities we had to be successful at to deliver, you know, on live account that interim, you know, kind of piece as well as the October 1st (inaudible).

BLACKBURN:
I yield back.

MURPHY:
I'm just curios to follow up to that. Did you ever present these concerns that you had about being ready with an (inaudible) running October 1 when you were interviewed by the McKinsey people?

CHAO:

Well, this was in the July timeframe. I think McKinsey was -- there interviews were in maybe March or April timeframe.

MURPHY:
I just wonder if you presented any concerns to them about being able to meet the stakes (ph) when you spoke with them.

CHAO:
I think it's a -- as a course of conducting project management, program management that working with CGI and QSSI and my team we discussed these concerns on an ongoing basis.

MURPHY:
I'll follow up.

CHAO:
OK.

MURPHY:
(Inaudible). Recognize Mr. Waxman for five minutes.

WAXMAN:
Thank you, Mr. Chairman. Nobody's happy with this rollout of the healthcare.gov and the administration is taking its lumps, but aside from lessons learned it seems to that my focus ought to be and my concern is getting this working. Americans want to be able to access the website and choose a healthcare plan, especially those who haven't been able to get an opportunity by health insurance in the past. That's why it seems to me if we need legislative changes, we should make changes to make it work, not to repeal it.

You know, the Republicans are so fixated on hating this law and they rather repeal it. They don't even want to consider helping make it work. And that's the focus that I want to use in asking you some questions, Mr. Chao. How do we make this work better? Now, is it accurate to say that CMS is getting the website up and running?

CHAO:
Yes.

WAXMAN:
OK. And is it accurate that CMS is cross -- Center for Medicare and Medicaid Services, that department part of the HHS is working at it, they have crossed 200 items off its punch list?

CHAO:
Correct.

WAXMAN:
And can you give me a few examples of important issues that have recently been addressed?

CHAO:
Issues related to the enrollment transactions that had some data issues, data quality issues that were fixed and now issuers can receive that data without doing a lot of cleaning up of that data. So the data quality is improved. The daily transactions that we sent to them have improved. The response times for the website have improved. The error rate of people experiencing some level of difficulty with moving from stage to stage in your online application, that has been reduced and improved.

WAXMAN:
Well, in fact, Jeff Zients's administration's point person on this whole website announced on Friday that you've dropped your error rate from 6 percent to below 1 percent. You've got the average wait time for page loading from eight seconds to less than one second.

What do these improvements look like to the average consumer going on this site?

CHAO:
I think it become transparent to the user. The user then can get at the task at hand of filling out their information, finding out if they are asking for a premium tax credits that they are calculated timely and they are proceeding ahead in the application so that they can apply some or none of that premium tax credit to their plan compare, so they can look at the offsets that occur and what the final premium should be to make their selection and to go the process in a very efficient and speedy fashion as compared to what they experienced on day one.

WAXMAN:

How about the overall stability of the site? It was down frequently in the early links. Has that improved?

CHAO:

Yes, certainly. I think we do have regular maintenance windows but those maintenance windows are used to implement these improvements that you've been hearing about.

WAXMAN:

So numbers seemed to be getting better and I expect we'll see more improvements. The anecdotal evidence I get is that the site is getting better slowly but surely. And that explains why the enrollment rate in November is speeding up significantly. In fact, I do have more than anecdotes. I have some figures in Massachusetts where they started a similar program. It started off slowly, only point -- 0.3 percent overall enrollees for private coverage signed up in the first month. And then, thus far, and the Affordable Care Act, 1.5 percent. So both started slowly. We even had what Massachusetts was. But after that, there was a surge in enrollment as people got closer to deadlines. The LA Times reported that, "A number of states that used their own systems are on track to hit enrollment targets for 2014 because of a sharp increase in November."

California which enrolled 31,000 people in private plans last month nearly doubled that in the first two weeks of this month. And several other states are outpacing their enrollment estimates. In Minnesota, enrollment the second half of October was triple the rate of the first half.

So we see an acceleration even in the federal marketplace. New York Times reported that the federal marketplace has nearly doubled its private plan enrollment in just the first two weeks of November. We're not what we need to be but we're seeing improvements. And this increased pace of people going back on the site successfully is to me very encouraging. So rather that just to (inaudible) care law and look for ways to undermine it, we ought to try to make it work and we're anxious to make sure that you do your job of getting that website and all of that working. And if we need any legislator change, call on us because we're ready, willing and able to act on that regard. I yield back my time.

MURPHY:

The gentleman's time has expired now. I recognize for five minutes the gentleman from Texas, Dr. Burgess.

BURGESS:
Thank you, Mr. Chairman. Thank you, and Mr. Chao for being here. In response to one of Dr. Murphy's questions about a breach in the system, you responded that you could not talk about it in open session, it would require classified briefing. Is that correct? Did I hear you correctly?

CHAO:
Correct. That's how I was instructed by our department.

BURGESS:
Very well. I would like to go on the record as I ask him (ph) the classified briefing with staff, bipartisan staff occurred. Can I get your commitment on trying to make that happen?

CHAO:
Yes, sir.

BURGESS:
Thank you. So the much talked about red team discussion document from the Washington Post this morning which, of course, you have not seen and I appreciate that. But you were interviewed in response to Mr. Martin's (ph) question. You were interviewed by the McKinsey team who were developing this?

CHAO:
Yes.

BURGESS:
Do you remember when?

CHAO:
Approximately April timeframe.

BURGESS:

During the timeframe that this was being developed. Do you recall what you talked about?

CHAO:
I think primarily, when I was intonating (ph) to the McKinsey team was a schedule challenge. Because during April we had just started QHP submission and working with issuers, they were very nervous that--

BURGESS:
Excuse me, what is QHP?

CHAO:
Qualified Health Plans.

BURGESS:
OK.

CHAO:
I apologize. And in -- during that month, it was a rapid, you know, a process to collect all the Qualified Health Plan data that you see in plan compare on healthcare.gov now as well as in the state- based marketplaces. And I was remarking on how that's unprecedented to only give issuers, you know, that short amount of time to submit your data and that we needed to make adjustments in the windows potentially so that they can come back in and make corrections. You know, that's an example of what I talked about in terms of the schedule challenges that we were trying to undertake something large scale, fairly complex compared to what's happening in the insurance landscape today. And that this was new and we were working on a short timeframe.

BURGESS:
And I will to stipulate that those are legitimate concerns. And so on page one of this red team document, at the bottom of the page highlighted, the working group determined that extending the go live date should not be part of the analysis and therefore work with a boundary condition of October 1st as the launched date. In other words, it didn't matter what the conditions on the ground were. Come hell or high water, October 1st, we got to go live. And were you given that impression by anyone on your team as you work through this?

CHAO:
Not necessarily characterized that way but as I mentioned ...

BURGESS:
Let me interrupt you because my time is limited, who would have made a decision like that? That it doesn't matter. I mean, it's like we all say it doesn't matter what - don't check the weather, we're flying anyway. Who would make a decision like that?

CHAO:
I think the decision ultimately is made, you know, by Marilyn Tavenner and, you know, team of folks, I'd suppose that she works with but as the administrator, she sets the deadlines for my work. And ...

BURGESS:
Does some of the people that are referenced in the report given to the committee by McKinsey that people that had discussions, White House, the old executive office building, people like Nancy-Ann DeParle, Jeanne Lambrew. Do you know if they were involved in these decisions?

CHAO:
I can't speak to that. I didn't hear anything about those discussions.

BURGESS:
Have you been in meetings with Jeanne Lambrew and Nancy-Ann DeParle?

CHAO:
Yes.

BURGESS:
And could you characterize those meetings?

CHAO:
The ones that I remember were dealing with coordination with IRS on their FTI, Federal Tax Information requirements, security protections and the Privacy Act with SSA.

BURGESS:
And any point during those meetings that it come up with the concern that we may not be ready trying to integrate all of these moving parts by October 1st.

CHAO:
Not in that context, no.

BURGESS:
In any context.

CHAO:
You know, concerns about whether if agencies are working closely together but not really in the context of October 1st, you know.

BURGESS:
One of the other things that keeps coming up and repeatedly in this report is that, number one, there is going to be there were no evolving requirements, there wasn't a consistent endpoint, there were multiple definitions of success, and in spite of all of the concerns brought up by the report, it must launch at full volume. I mean, almost sounds like a recipe for disaster, doesn't it?

You're changing the definition as it goes along. You are not allowed to change the date and you got to launch at full volume. That's a pretty tall (ph) order, isn't it?

CHAO:
It is.

BURGESS:
But let me ask you this. How does it make you feel to know that there was this kind of report up there and then other people knew about it, people in the White House, people within the agency and you've been the primary point man out there and no one discussed it with you? How does it make you feel?

CHAO:

I'm actually not terribly hurt by it or surprised by it. I think the information contained within it is something that I live on a day to day basis to try to deliver a working system.

BURGESS:
You're playing into everyone's works here about what it's like to be in the bureaucracy. Let me ask you this. One of the things brought up in this report is that there is not a single implementation leader ...

(UNKNOWN)
That's right.

BURGESS:
Do you feel during you time that there has been a single implementation leader that you could look to for advice and direction through this?

CHAO:
I think I'd look to several because of how ...

BURGESS:
Name one.

(CROSSTALK)

MURPHY:
... need to follow up with that. So let's submit those questions for the record to. Now I recognize the gentleman from Texas, Mr. Green, for five minutes.

GREEN:
Thank you, Mr. Chairman. Like all of us, I have so many concern, ask some questions in the minute about the healthcare.gov, but I wanted to just say that, you know, it is frustrating for those of us on this (inaudible) who supported it, who actually worked a lot of times on the drafting of different versions of the Affordable Care Act to see what happen on October 1st without the roll out. And (inaudible) as successful that's why we need to deal with it because having been here through also the Prescription Drug Plan for seniors, that's the way you can get to the numbers you really need. So hopefully, that will happen.

But the law is still there, and last Saturday in our district (inaudible) Houston because in Texas we unfortunately, we have some the highest percentage and numbers of uninsured folks in the country. In our congressional district, 42 percent of my constituents work and don't have insurance to their employer. So they could -- they would be qualified to go to with the ACA, and we actually didn't taper. Now, I have to admit, I can't remember except (inaudible) around when Medicare was rolled out, I guess, that was the last time we rolled (inaudible) by taper.

But let me give you the results. We have three members in Congress. The mayor of Houston, our republican county judge and the Secretary of Labor, we actually had 800 families show up on a Saturday morning and signed in, of course, with multiple attendees per family. Nearly 300 people set up -- follow up appointments after a navigator. We had 88 of the certified navigators there and we don't know how many applications were completed because the number is still being tallied by navigators and HHS in our regional office out of Dallas.

So there are people out there who want to do it. And if we have to do it by paper, we will do it. But that's the frustration we have. We want this to work because there are millions of people in our country who need this. And I know the majority in the house may not understand that but I know in our district they do. But I don't know if you have a comment but let me -- then I can get to the -- the healthcare.gov.

CHAO:
I think CMS takes to heart the matter and I think everyone working on this is actually serious about improving this experience because we know that in districts like yours, there are quite a few number of people that need and want to enroll and use this benefit. So we are certainly working very hard to make that happen.

GREEN:
Well, with that success, believe me, we're going to do a lot of smaller ones in our district in trying to work with and partner with media companies that maybe get to message out. I have a few questions about healthcare.gov and the important goal. I think we both share in sharing this part of the success and implementation by the Affordable Care Act. People find access to care they need and when they need it. Part of this goal requires the federal and state exchange to secure the American people can trust their information and privacy won't be compromised.

How is the data hub used to determine eligibility and enroll applicants and process appeals different from the data system used by other agency -- federal agency such as Social Security or the IRS.

CHAO:
How is the data hub different?

GREEN:
Than the other agencies. There are obviously have up and running ways with Social Security and even IRS.

CHAO:
I think what makes it different is that, for example, SSA is the eligible agency for Medicare. So every night, SSA's field offices load data about accretions, depletions into the Medicare program and we receive a very large file from them every night that we process for two to three hours to update all of our systems so that providers can see new Medicare beneficiaries accreting into the system. That's lots of data moving between two organizations and it's stored and it is time intensive.

The data services hub goes out and for a requester of that data, a valid requester, it reaves (ph) the data where the sources transfers it back to the requester in a secure fashion, does not remember the contents of that data and facilitates that without moving massive, you know, millions of records of data all at once, all the time everyday. It only transfers enough data to get the job done.

GREEN:
Were you at HHS, when we've gone through to Medicare enrolling back internet? I mean, when we shifted from having going to the Social Security office about the paperwork. You can do online now.

CHAO:
Yes, yes.

GREEN:
And I assume there were some glitches when that first started.

CHAO:

Yes.

GREEN:
And, of course, we didn't have a deadline and a roll out and things like that. It was built in over the time, so you had time to problem solve. And our problem is we don't have that kind of problem solved here in later November.

CHAO:
I still remember in the mid-'90s, SSA put up the electronic benefits statement and after a few months, they had to take it down and then they didn't come back up until years later so they perfected it.

GREEN:
Thank you, Mr. Chairman.

MURPHY:
Gentleman yields back. I now recognize the gentleman from Louisiana, Mr. Scalise, for five minutes.

SCALISE:
Thank you, Mr. Chairman. I appreciate you having this hearing and Mr. Chao, I appreciate you coming to testify before us. We had a number of hearings like this over the last few months trying to find out first how the roll out was going to work and, of course, but we've gotten testimony time and time again from the administration that the roll out was going to be fine.

And then, I think what's most frustrating is that when this report came out, this McKinsey report that really chronicles the problems that were happening months ago or back in March and April at the same time that administration officials were telling us that everything was going to be fine. And so that in telling American family that everything was going to be fine or when October 1st hit. I guess there are many things about this that trouble me but first, you know, when I look at this, you say you hadn't seen this report. And I've read through a number of these items that McKinsey pointed out in the report that they were telling to somebody in CMS around you, over you, under you, somewhere but the other things that should have been just basic testing requirements, you know, I used to write software, I actually wrote test plans for software roll outs and, you know, in fact many of these is just basic

comments and things you do. I mean, if we may -- one line of code change we literally would test that over and over in multiple ways (ph) let alone major changes. What this report talks about is chaos at CMS. Nobody's in-charge.

They talked about the fact that you had multiple people that were making multiple changes to a major design change to the system, just weeks prior to the testing, I mean, prior to the roll out without testing it. I mean did you have a test plan? Did you -- whether you're not -- you read this report, these are things that you should have been doing anyway. I mean, we're you all making changes, big changes all the way through and were you testing any of those changes? You'd say, "Well, you know, they told us October 1st, roll it out no matter what."

CHAO:
You've asked a lot of questions in there.

SCALISE:
Yes.

CHAO:
So let me try to recall how to address them. I think that's certainly yes. If you have this experience in software development, you need to have solid requirements before you can actually have good test cases in which to actually run test. I think it's a dynamically changing environment of which if we had more time and we -- and the time would have been devoted to solidifying requirements that are translated from policy.

SCALISE:
Yes, three years. That was three years. This was -- this isn't something that just kind of got flopped on your desk. I mean, the law passed and (inaudible) the law in 2010. There was a lot of time to prepare for it. The requirements, a major requirement for change in weeks before some of them for political reasons by the Obama administration. So you can't just say, "Well, you know, we just didn't have enough time." I mean somebody in CMS and if it wasn't you, it was (inaudible) or Ms. Tavenner who knows who it was. And somebody was making all these changes and saying, "Gee-whiz" I mean, you know, we've -- lots of (ph) make big changes and don't test it because we want to roll those things out no matter what.

CHAO:

Well, having written software or written test cases, you know that the requirements come from the business side or the policy side. And they're subject to change based upon how your customer or your ...

SCALISE:
The law didn't change. The law was passed and for three years that law didn't change. The law was there. You know what those requirements were. If you make changes in your requirements, you also ought to make changes in the passed plan.

CHAO:
And the law is a very high level expression of requirements that certainly you can't develop code or test cases from -- there needs to be a significant amount of translation into lower level details. And that's what I mean by a schedule of challenges that we have to receive those requirements and translating them into test cases -- test data to exercise the system and as well build the system, too.

SCALISE:
You know what, they talked in this report that the contractor receives absolutely conflicting direction between the various entities within CMS, conflicting directions within CMS, that's not or requirement change as one person saying do this and another person in the same agency saying do something indifferent. And by the way, none of that's being tested in the meantime. That's not evolving requirements, that's chaos within the Obama administration where they're literally changing things and multiple people are changing them and nobody's talking to anybody.

CHAO:
I can't speak to how they characterized it but -- but I think that in CMS we have Medicaid and Chip requirements, we have insurance exchange requirements, oversight requirements, medical loss ratio, rave review early retiree reinsurance.

SCALISE:
And I know you have a lot.

(CROSSTALK)

SCALISE:

The bottom line is -- the bottom line is this report lays out the chaos that was going on but these -- all of this information was known within the White House. Reports were being briefed to people in the White House. And even President Obama didn't know about it in which case people directly under him knew that this thing was going to be a disaster, you just didn't tell him or the President did know about it, went out misleading people anyway. But he had a way. If the President really didn't know about this, this report says the White House absolutely knew what was going on and they didn't tell the President. He ought to be firing these people today.

If somebody at the CCIIO went out there and said, "I'm rolling out this project." This is going to be just like buying a TV on Amazon. That's what the President said, and if somebody right underneath him knew that it wasn't going to be like that, and this report says absolutely they knew and they didn't tell the President, he ought to go and fire every single one of those people right now and hold them accountable or maybe that just says that he did know about it. And mostly, what the President says that this report is damning (ph). I yield back the balance of my time.

MURPHY:
Gentleman's time has expired. I just -- can you just clarify an answer you gave to the gentleman here. I thought you said something like, with more time you would have done more testing or something on those lines. So you're saying, you would have liked to have more time?

CHAO:
No, I think that's what I mean by there's a schedule of challenges that you're trying to maximize the time that you have left as you're trying to extract the requirements from the policy that's being finalized. The longer policy takes to be finalized, the longer it takes to translate ...

MURPHY:
You wish you would have had more time to test it?

CHAO:
I think that's true of every project I've ever worked on.

MURPHY:
Thank you. Now, I recognize Mr. Yarmuth for five minutes.

YARMUTH:
Thank you, Mr. Chairman. Thank you, Mr. Chao, for your -- your testimony today. I just want to follow up a little bit on Mr. Scalise's line of questioning. The issue whether or not you had three years to prepare for this, when was the deadline for states to decide whether they were joining the -- doing their own exchanges or were going to participate in the federal exchange?

CHAO:
I think the timeframe was the end of 2012.

YARMUTH:
End of 2012. So January 1st essentially of this past year. And when was the deadline for states to decide whether they were going to enter into a partnership with the federal government?

CHAO:
I believe it was the end of April 2013.

YARMUTH:
So really the Department did -- or CMS did not have three years to prepare and there was probably no way to guess (ph) three years ago that only 14 states in the district of Columbia were going to set up their own exchanges. Wasn't the anticipation that far more states would do their own exchanges?

CHAO:
Yes, we were hoping so.

YARMUTH:
So it really wasn't until this year that CMS really understood the magnitude of the volume of work that the website was going to have to accommodate.

CHAO:
Correct. Not such a clear binary decision. You do or you don', there's still coordination that has to occur in (inaudible)

YARMUTH:

Right. Thank you for that. You know, obviously, when we're talking about security, we're talking about two separate issues. One is the vulnerability of the system to some kind of outside attack. I don't know why anyone would really want to attack the federal exchange but some (inaudible) is an issue. The second one is the average citizen is concerned about the information that has -- they are about now. And I think that's one thing we're most interested here.

Mr. Dingell actually asked you directly about the fact that there really isn't very much information on the website that would be considered (inaudible) in nature. And I guess the question I want to ask is, are people who are working with the exchange now subject to or vulnerable to a more a breach of their privacy than they were under the prior system when the insurance companies had pages and pages and pages of health information including every doctor they had ever visited, every prescription they had ever taken, every medical procedure they had undergone over a certain period of time? Would you say that there was much more vulnerability under that system than there would be the federal exchange?

CHAO:
Much more so because so much more personal information including health information was involved in that process.

YARMUTH:
And I think during the course of questioning, we've actually done a pretty good job of debunking with the issue as to whether there really was a security problem here. There was no evidence that there has been. And I think there really hasn't been any evidence presented that would make us doubt that. So I'm glad about that. And I think that should encourage Americans to participate more actively.

And since one of the things that's come up and it involves the question of 80 percent, and that is something I want to clarify because the press reports have been that the administration had set as a metric, that 80 percent would be able to get on the site and smoothly sign up and enroll for health coverage as of the end of this month. That doesn't mean that the remaining 20 percent won't be able to access affordable quality health insurance (inaudible).

CHAO:

No, I can't speak to the exact percentages but I think there is a recognition that some people, whether at the healthcare.gov or any system, for example, if you walk into an SSA field office, how many people can actually get their business done in one visit as compared to, you know, the greater majority of people. I think some people need extra help. They need assistance to navigate the process. And I think that that's probably what you were referring to.

YARMUTH:
Thank you very much for that. And I just want to do some shameless self-promotion for my state right now. As of last Friday, Kentucky obviously is operating its own exchange, 48,000 Kentuckians are enrolled in new health insurance, 41 percent of them are under the age of 35, over 452,000 visitors have gone to the website, 380,000 people have conducted preliminary screenings to find out if they're eligible for coverage. And I think, most importantly, maybe over almost 1,000 businesses have actually begun the process of signing up for a new coverage to their employees. And over 300 have actually been enrolled and have been qualified now to offer coverage.

So Kentucky is doing well and I hope the federal exchange will do just as well. I yield back.

(UNKNOWN)
Gentleman yields back. Now, I recognize Mr. Harper for five minutes.

HARPER:
Thank you, Mr. Chairman. And Mr. Chao, thank you for your time here today. And you replied earlier on a follow-up question that the Chairman had. I believe you said you would like to have had more time for the testing. Did you request more time from anyone?

CHAO:
No.

HARPER:
And can you tell me why you did not request more time?

CHAO:

Because I was given a target of October 1st and various other delivery dates which I had to stay on schedule for.

HARPER:
Do you believe it was ready for October 1st?

CHAO:
I believe we did everything we could to make sure that the right priorities were set so that we could deliver a system on October 1st.

HARPER:
And do you believe the system was delivered on October 1st?

CHAO:
It was.

It wasn't performing as well as we like and certainly had more glitches than we anticipated but we did deliver a system on October 1st.

HARPER:
Do you think glitches is the proper word to use to describe the roll out?

CHAO:
I think there are problems, there are defects, if you, you know, glitches is just a word that's commonly used right now.

HARPER:
Well, glitches doesn't seem to convey how serious the failure of the roll out has been and so here we are. And, of course, one of big the concerns that we have is what do you do about making sure that personally identifiable information for those who signed up is protected? And on the report that you have, there on page 11, if I can get you to take a look at that real quick on the McKinsey report.

In the bottom of page 11, it says, and, of course, at the top, it says options that could be implemented to help mitigate key risks. At the bottom it says, name a single implementation leader and implement associated governments process. Has there been a single implementation leader named?

CHAO:
I don't think that's the way it's been characterized before, but I think Marilyn Tavenner, our administrator certainly has accepted accountability and she does run the agency ...

HARPER:
Certainly, but that's not saying that she is supposed to be the single implementation leader there. Is that how you read that report?

CHAO:
(Inaudible) again. I didn't see this until just this very minute. So I ...

HARPER:
You know, I've spent some time here while we're waiting on a time to question here. I went to the healthcare.gov site and it took a little while to try to figure out how (inaudible) search to get to the information of how you protect yourself from fraud in the health insurance marketplace. And if you -- and it's takes a couple steps to get to this information. So people probably more sophisticated than I am on this would need to be tracking this.

But if you look at it on the side, it says, "How to report suspected fraud." And it said you can report suspected fraud in one of two ways and it lists a breakdown of one way which is to use the Federal Trade Commission's online Complaint Assistant. And I've tried that a moment ago and it was not very successful, it says you can call your local police department. And then it says you can visit a site, the Federal Trade Commission to learn more about identity theft.

And the second choice is called the Health Insurance Marketplace Call Center, and it gives that number. So if you were the victim of personally identifiable information being fraudulently released or obtained, who would you call first under that stereo?

CHAO:
All right, the listed call center number, the marketplace call center ...

HARPER:
And if ...

CHAO:
... if you're in a federally facilitated market.

HARPER):
OK, and it says, "Explain what happened and your information will be handled appropriately." How do you define handled appropriately? What is that? How do you get someone's identity back once it's been compromised or there's been an identity theft?

CHAO:
Well, I think there needs to be some analysis and collection of information to make sure what type of situation occurred and then make a decision going forward here.

HARPER:
Well, obviously this is a critical matter, so some determination made -- what's the timeframe? How quickly can someone's life be put back together if this were to happen?

CHAO:
I think it's situationally dependent and I really can't -- I'm not comfortable (inaudible) answer right on.

HARPER:
You have said early that steps were being taken to prevent unauthorized access to the sites. What about those who may have authorized access but released (ph) it in an authorized manner? What protections or safeguards put in there particularly for those with the navigators and -- in a situation that there's been no background check unless it was required in the state? How is that being handled with the use of navigators?

CHAO:
I think the premise is that when we issue, for example, a grant to a navigator or organization or we sign a computer matching agreement with a state (ph) that there are rules, behavior and certain any kind of requirements that are associated with signing that agreement or receiving that grant.

HARPER:

Do you have a central reporting location of the navigators that are in violation or reported in violation?

CHAO:
I have to check on that.

(CROSSTALK)

HARPER:
You let us know. And my time has expired.

MURPHY:
Thank you. Mr. Long, I recognize you for five minutes.

LONG:
Mr. Chairman, thank you so very much. Mr. Chao, you were just presented with a whole series of hypotheticals. Have any of those hypotheticals happened?

CHAO:
No, not to our knowledge, no.

LONG:
I appreciate that. And I would suggest, Mr Chao, if someone was maliciously using information in a way what they were not allowed to use it, would that be a crime?

CHAO:
Can you repeat that question again?

LONG:
If someone hacked into the website and was using information in a way that they weren't allowed to use it, so in any way, wouldn't that be considered a crime?

CHAO:
Certainly, yes.

LONG:
And I believe that we would fully prosecute those individuals?

CHAO:
Yes.

LONG:
And I would hope that this Committee will fully support and encourage the Department of Justice to go and fully prosecute anyone that's hacking this website.

Mr. Chairman, it wasn't too long ago that there was a hearing that this Committee had on Lifeline (ph). And there was -- some of my republican colleagues were encouraging members -- citizens of the United States to go to visit obamaphone.net to sign up for a Lifeline (ph) or to get information from the website as to the accuracy of what the program was about.

An hour later the website was taken down and this Committee, myself and Congresswoman Eshoo (ph) asked the FCC to look into the matter but they said it appears that, you know, (inaudible) way that this data was being collected but the website is now down. I think we, as members of Congress need to be careful with how we're reporting information on to the American people. We need to be careful about this.

There's not again a member on this Committee that doesn't believe that we should get the website working, that we need to get to facts of what's happening, and with that being said, Mr Chao, I guess two things, Mr. Chairman, there is a GAO report that was published on April 24th of 2012 entitled, Cybersecurity: Threats Impacting the Nation, and I'd like to ask (inaudible) to the record.

The report, and I'd invite everyone in the Committee to take a look at this. It was -- Homeland Security Department or Committee talking about the threats that our nation is facing. The Intelligence Committee, Homeland Security, the White House, Members of Congress websites have been hacked into. We need to do more in this area to make sure that we're keeping information secure.

But with that being said, Mr. Chao, this has been talked about a bit but on the front page of the Washington Post this morning, there was an article about a document that was linked to the paper by the Committee Majority. The article describes the analysis conducted in 2013 by McKinsey and

company with identified potential risk with the development of healthcare.gov. The report shadows some of the problems that we now have face today. Mr. Chao, did you see the report at the time that was published in March and April of 2013?

CHAO:
No, I did not.

LONG:
So is it fair to say that you are the best person to comment on why the report was done and how CMS and HHS responded to its findings?

CHAO:
Yes.

LONG:
Mr. Chairman, I raised this because it illustrates a number of problems with how this has been handled. In particular, the perception that's created when you withhold documents from the democrats and the Committee and when you play Gotchi games (ph) by leaking material to the press without context, it makes it appear that you're more interested in running a partisan investigation than in finding the facts. And I certainly hope that that's not the case and believe that not to be true. But we need to work together to get to the bottom of this.

So with that being said, Mr. Chao, what efforts is the Department of Health and Human Services undertaking to address the ongoing threats?

CHAO:
We listed as part of our mitigation strategy daily and weekly security testing and scans, which is something we always do, but in this case we do it more frequently because we understand the sensitive nature of healthcare.gov and the trust and confidence we have to obtain from people to come and use the site.

LONG:
And how is the department coordinating with other federal agencies who maintain (ph) websites that also gather personal information?

CHAO:
I think we work with all of our key partners that are connected to the hub to make sure that we function under what we call a Harmonized Privacy and Security Framework and along with the states, have a process and a program in place to handle certain situations in which there are incidence that need to be managed about the potential data breaches. So we have a program, we have a policy, we have several operational procedures in place -- work and coordinating across all the agencies.

LONG:
And does that include, Mr. Chao, the Intelligence Committee or the Department of Homeland Security?

CHAO:
Yes.

LONG:
Very good. So with that, Mr. Chairman, as I yield back my time, I just hope that it's clear, Mr. Chao, to you, to the President that we're not happy with the roll out right now. We need to get this working. There's too many vulnerable Americans that need access to care and we need to make sure that we can get them that coverage in the same way protect the information. But I think it is big step forward. They no longer -- will individuals have to report the kind of illnesses or accidents that they've had in their past so they can get care in the future. And with that, Mr. Chairman, I yield back.

MURPHY:
Gentleman yields back and without objection. And the gentleman's document will be submitted to the record. Now, Chair now recognizes the gentleman from Colorado, Mr. Gardner for five minutes.

GARDNER:
Thank you, Mr. Chairman and I thank you, Mr. Chao for your time before the Committee today. Last week, the President met with several representatives of the Insurance Industry to discuss solutions that may be possible in light of the healthcare.gov debacle. Have you had any conversations about changes you can make to healthcare.gov to assist the insurance industry?

CHAO:

I think part of the strategy, I haven't spoken to the insurance industry myself or have been part of those meetings, but I think as part of the strategy under Jeff Zients's is to improve the experience of consumers but that involves, you know, key -- certain parties that are also a key to this equation of getting enrolled with those agents and brokers and working with issuers to fix certain aspects of the systems to make it work better ...

GARDNER:
So you had any discussions then about providing insurance companies with the ability to directly enroll or anybody in your department?

CHAO:
We had designed something called Direct Enrollment into healthcare.gov or a part of that FFM (ph) system architecture to accommodate that.

GARDNER:
And so that's -- and that feature has been turned on or it has not been turned on?

CHAO:
It was not working well and then initially, like many other things, but have been performing fixes and optimizing it and working with issuers to get direct enrollment ...

GARDNER:
So you've had any discussions on giving insurance direct acces to information on eligibility for subsidies?

CHAO:
Only in terms of the results, but there is a series of (inaudible) security ...

GARDNER:
Hand-offs.

CHAO:
Yes, hand-offs.

GARDNER:

That's a yes, then?

CHAO:
Yes.

GARDNER:
OK, thank you for that. Do you -- going back to the question about the feature (inaudible). Will that happen in the future, then, to that question, discussions about giving insurance direct access to information on eligibility for subsidies, do you believe that will happen in the future?

CHAO:
It's not really direct access. It's more of a hand-off, a secure hand-off in which they've collected enough information about the applicant and, you know, or an agent and broker and this person has given the authorization for a consent to work with them as a third party.

GARDNER:
So that's a yes, then, again as well?

CHAO:
It's not access to eligibility data. It is a more involved process that protects that person's information.

GARDNER:
But they'll be getting their information -- insurance company will be getting the subsidy to access.

CHAO:
They don't get the calculated. We -- that is a marketplace ...

GARDNER:
But they'll have information on eligibility for the subsidies directly?

CHAO:
Only as a result of the marketplace handling a data, not touching that eligibility themselves.

GARDNER:
The Committee has been reviewing materials that indicate that some parts of healthcare.gov were not completed before the launch as we discussed here. What portion or percentage of the website remained to be created when we launched on October 1st?

CHAO:
I don't have an exact percentage. I think some of the previous conversations when people ask about whether if things were complete. I look at it in terms of over all marketplace systems ...

GARDNER:
We've never talked about what's complete, what's not complete, whether it's how much ...

CHAO:
I think it was just kind of priority functions that need to be in place, like for example, you had to authenticate an individual, that's a key function that had ...

GARDNER:
Well, how much do we have to build today, still? I mean what do we need to build, 50 percent, 40 percent, 30 percent?

CHAO:
I think it's just an approximation, we're probably sitting somewhere between 60 percent and 70 percent because we still have to put the system ...

GARDNER:
60 percent or 70 percent that needs to be built, still?

CHAO:
Because we still have to build the payment systems to make payments the issuers (ph) in January.

GARDNER:

Let me get this correct, 60 percent to 70 percent of healthcare.gov still needs to be built?

CHAO:
It's not really healthcare.gov. It's the federally- facilitated marketplace ...

GARDNER:
But the entire system that the American people are being required to rely upon, 60 percent to 70 percent ...

CHAO:
That part -- healthcare.gov, the online application, verification, determination, plan compare, and getting enrolled, generating enrollment transactions, that's 100 percent there. What I'm talking about ...

GARDNER:
But the entire system is 60 percent or 70 percent away from being complete?

CHAO:
There's the back office systems, the accounting systems, the payment systems, they still need to ...

GARDNER:
How -- of those 60 percent to 70 percent of systems that are still being built, how are they going to be tested?

CHAO:
You mean, the remaining ...

GARDNER:
Yes.

CHAO:
... 30 percent to 40 percent? How are they going to be tested?

GARDNER:

Yes.

CHAO:
In the same exact manner we tested everything else.

GARDNER:
Is it difficult to review the new parts of the website while it's operating?

CHAO:
It won't affect the front end -- the front parts ...

GARDNER:
But that's pretty difficult, isn't it?

CHAO:
Excuse me?

GARDNER:
It's pretty difficult to review it while it's in operation, correct?

CHAO:
No, it doesn't involve the front part ...

GARDNER:
Right, but where it's operating, is it ...

CHAO:
... when we are trying to calculate a payment, derive a payment, do data matches on the back end, that doesn't affect the healthcare.gov operations.

GARDNER:
How long will you have to test those parts that you're building?

CHAO:
They are an ongoing basis, depends on their build schedule.

GARDNER:
So is it appropriate given the performance of healthcare.gov where we're at right now to launch any new applications or features about testing them heavily before they go live?

CHAO:
We are testing.

GARDNER:
Mr. Chairman, I have several of the questions and we'll follow up with you, but thank you for your time.

MURPHY:
Thank you. Now, I recognize Mr. Welch for five minutes.

WELCH:
Thank you very much. Thank you for the hearing. There is a mutual desire to get this thing to work. And there's really two models that we can use to deal with the failed roll out. One is to fix it and the other is to use it as (inaudible) to relitigate the battle about whether healthcare is the law of the land.

And my hope is that we'll pass that. There's an absolute urgency to make things work. And I know, Mr. Chao, that's your job. And I just want to put this into context. We had a big battle in this Congress. I was not here over the passage of Medicare Part D. It was a largely a partisan vote. The republicans under George Bush were for it. Most of the democrats we're against it but it passed in a very close intense vote. And in my understanding is that it then went into the implementation phase which required the computer program in a website. There were lots of significant difficulties with that program.

And there were concerns about having it work. And I just want to ask you a little bit about that history so that we have a context of the challenges we have today. And not at all as an excuse because there's real unity about meeting to get this fixed. But is the actions we take -- are the actions we take about getting it fixed or about trying to derail and scuttle the overall healthcare program. America is going to have to judge. But can you give us a sense what was going on inside the agency when you were preparing the Medicare Part D website in 2005? And were there concerns and issues that needed to be addressed then?

CHAO:
The biggest and most prominent example that I can recall was the concern around auto assignment and auto enrolling Medicare -- Medicaid full benefit dual eligibles to receive a Part D prescription drug benefit and switching them over as of January 1st. And that's -- we had sent these enrollment files out to the plans, the health plans were part D sponsors around November. And in December, it was some realization, you know, last minute realization then, pharmacist and pharmacies were -- who are in the front line of helping these beneficiaries required, you know, some access to the information to help them navigate this new change.

So as an example, we scrambled and we developed a method for pharmacies to actually get access to authorizations to Medicare enrollment data for the dual eligibles that were enrolled so that at point of sale, they can at least do things such as, you know, three- day (ph) sales ...

WELCH:
Right.

CHAO:
... just to figure out what plan they might be in. And, you know, that's just an example I recall that was a mass scramble, time crunch, how to get it in place. Lots of, you know, working around the clock, lots of urgency, pushing many, many people not just on the contract or in the staff side but working with the prescription drug industry as a whole including pharmacists to make this happen.

WELCH:
All right. And those problems continued even after the January 1 roll out date in my understanding?

CHAO:
Correct, because it's not perfected. It's -- it's got so much technical issue when you introduce a new business process, for example, in the procedures, you know, in administrative aspect of healthcare. It takes a while for people to actually understand how that works, you know, as compared to learning the data system that's involved to support that business process. So it's more than just a technical issue.

WELCH:
OK. And is it your view that as to we ultimately succeeded with Part D, we can ultimately succeed in terms of the technical -- the website issues with healthcare.gov?

CHAO:
Certainly. I think it comes with being focused and driven to get at the root of the problem and to fix the systems because on the technical issue side, it is solvable, very solvable. And we've shown that it's made improvements.

WELCH:
OK. Thank you very much. I yield back.

MURPHY:
Gentleman yields back. And now I recognize for five minutes gentleman from Virginia, Mr. Griffith.

GRIFFITH:
Thank you, Mr. Chairman. Now, speaking of Medicare Part D, no one was required by law or force of penalty to subscribe to that, isn't that correct?

CHAO:
No. But we did auto assign auto enrolled Medicare -- Medicaid dual eligibles into Medicare Part D.

GRIFFITH:
But it is a different animal than what we're dealing with now because lots of Americans were being in told they can't have their insurance. So they're going to have to sign up through the exchanges. So I do appreciate that but there is a difference.

You know one of the things that when you get a time to take a look at the report. And I think it's a symptom of the problems that this website had had is that you were not included in the briefings on the report that has come to light in the last 24 hours. But when you get a chance to read that, one of the things you'll see is they thought there ought to be one person overseeing all the different parts in listening to the vendors who'd previously testified before this Committee. It looked like they reached build in their own part and then in the last months, they had to squeeze it all together, in the last two weeks things were changing.

Another part of that report shows us that on the timeline, you really want to have your -- you want to define your policy requirements prior to finishing the design and starting to build, wouldn't you agree with that?

CHAO:
That is the logical thing to.

GRIFFITH:
It is the logical thing to do. But in reality, we've heard testimony in this Committee that they were changing policy. We know that the big change on July the 2nd when all the sudden the employer mandate was illegibly delayed. The president signed an executive order -- I'm not sure it has legal authority, but you did that, delayed that employer mandate further we know from testimony that there were changes being made as close to the launch as two weeks before. So based on that, it is -- it would be the logical conclusion that you're going to have significant problems, wouldn't it?

CHAO:
With the luxury of hindsight, I can see that, you know, there are contributors to the way the system performed when it was unveiled. That's not, you know, I need to focus on fixing this thing ...

GRIFFITH:
And I know that your focus is to fix it now but also when you take a look at it, when you're still defining your policy requirements as late as two weeks prior to launch, it's very difficult to design and then to build and then to test a system and have it work whether it's the security component or the performance component. It would be logical to do it in the proper order when you do the illogical, you're liable to have problems. I know you would agree with that if you were free to answer honestly.

And I would say to you that I also noticed that they never, nobody -- no one person was ever appointed to head this up while you were in charge of part of it and you're in charge making part of it work. It looks like there is at least six different representatives from different agencies that had a hand in overseeing what was going on and no one had control over the others. Isn't that correct?

CHAO:
I think it was a governance committee that was formed.

GRIFFITH:
A governance committee. And, ain't that interesting. And sometimes when you try to launch big projects like this, so you have to have one general in charge of the operation, wouldn't that be logical?

CHAO:
I would say that for the technical pieces, you know, I was responsible for making sure that the second pieces were organized.

GRIFFITH:
All right. And last month, this Committee uncovered a September 27 memorandum indicating that healthcare.gov launched without a full security control assessment. Administrator Tavenner had to attest that she was aware that the launch carried security risks. Can you tell us what those risks are specifically?

CHAO:
I -- first of all, I think the incomplete testing. It was fully security tested to three rounds of testing, so that when we -- when Marilyn Tavenner signed the authority to operate on September 27th, it had no high findings and had gone through the appropriate security testing.

GRIFFITH:
So you didn't -- so what she said was not accurate that it had a -- did not have a full security control assessment. She was mistaken when she testified in front of this committee ...

CHAO:
I think there's a part of that sentence that might be -- it needs clarification. I think what we we're trying to say was that the security control assessment was not tested for a full entire system of which we were still -- remember, we're still building financial manager and aspects of it. I think it was just an acknowledgment that 100 percent of the system was not complete at that time.

GRIFFITH:
OK. And it's still not complete today and the people of America want to know, you know, what's the security going to be if it's not complete on January ...

CHAO:
... the October 1st pieces that were necessary such as insurance security privacy for those functions that I have mentioned were tested.

GRIFFITH:
And I appreciate that. What can we expect in January 1? I apologize, I yield back.

MURPHY:
Thank you, and by the way our prayers are with the family of State Senator Creigh in Virginia who is I guess in critical ...

(UNKNOWN)
If I may -- since you bring it up. If I may take a moment of personal privilege, I do appreciate your prayers. Creigh and I were on in opposite parties but just like on this Committee, you form friendships and he served with me in that Virginia House of Delegates before he went on to the Senate and went on to run for other office. But he is still sitting senator and it obviously has shaken everybody in Virginia. And he is a good man. Our prayers are with him and I encourage everybody to say a prayer for Senator Deeds and his family.

MURPHY:
Thank you. Gentleman. Now, turning to Mr. Tonko for five minutes.

TONKO:
Thank you, Mr. Chair. I'd like to continue on that recent questioning of the documents -- document that my republican colleagues have released. Mr. Chao, this document was signed, I believe, on September 27th, and it's an ATO, an authority to operate memorandum to operate the federally-facilitated marketplace for six months and implemented security mitigation plan. Can you tell us, are ATOs commonly used in federal data systems?

CHAO:
Yes. It is in essence the last official sign-off to authorize a federal system to go into operations.

TONKO:

Thank you. And can you tell us why Administrator Tavenner signed this ATO rather than perhaps other officials that might report to the administrator?

CHAO:
I think the span of the stakeholders that were involved across the agency has -- we have not had a system that had this unprecedented involvement of so many different components so that the recommendation by our chief information officer was to make a recommendation for the administrator to actually sign off on this because she runs the entire agency.

TONKO:
And the fact that she signed it is good news? It's an indication I would believe that officials at the highest level of CMS were briefed on and taking responsibility for site security?

CHAO:
Correct. Yes.

TONKO:
Now, as I understand that this document describes security testing for the healthcare.gov website, it says that security testing of the marketplace was ongoing since its inception, and into September 2013. In fact it says that and I quote throughout the three rounds of security control assessment testing, all of the security controls have been tested on different versions of the system. Is that correct?

CHAO:
Correct.

TONKO:
I (inaudible) goes on to say that the cost (ph) of system readiness and complete security assessment of all the security controls and one (ph) complete version of the system was not performed. So it's that (ph) this lack of testing, and I quote, exposed to level of uncertainty that could be -- has a high risk.

CHAO:

I didn't actually -- I had recommended, as part of that decision memo and I think at that time, as I mentioned earlier, you know, it's semantics, you know, not 100 percent of the system was built so you can't really consciously say you have it all available in one place to fully test because not everything was needed for October 1st. Only essential pieces involving healthcare.gov were tested for security (ph).

TONKO:
So the document then indicated that CMS postponed the final security assessment screening, right? And the -- in its place, CMS, did put in place a number of mitigation measures. And it concluded that these measures would mitigate the security risk. I want to take a moment to ask you about the September 27th ATO and how the risks identified are being addressed. Can you describe the recommendations in that September 27th memo?

CHAO:
You mean, in terms of mitigations?

TONKO:
Yes.

CHAO:
OK. So on a daily basis, we run antivirus scans every three minutes. Now we run scans every three minutes. Data full monitoring is a continuous effort. Direct protection analysis against known bad IPs or hackers, I've mentioned that in the opening remarks, that it's continuous. On a weekly basis, we monitor operating system compliance, infrastructure system compliance, we conduct penetration testing authenticated and non-authenticated by marketplace security teams. We have a 24 by seven security operations team. We conduct additional penetration testing, authenticated and non-authenticated by another group of security professionals in CMS that report under our chief information security officer. We also conduct application software assurance testing which is occurring biweekly. And on a monthly basis, we produce a plan of actions and milestones that keeps track and reports on any discovered weaknesses during all this monitoring.

TONKO:
So, CMS is taking action that was recommended in the ATO.

CHAO:
Correct.

TONKO:
And do you have confidence in these and other measures you are taking to protect the security of Americans' personal information?

CHAO:
I'm high confidence.

TONKO:
OK. As I understand it here, the remedial actions and the ongoing security testing are protecting the security of the website.

CHAO:
Yes.

TONKO:
And so, perhaps, the message coming from our republican colleagues is that they do not want the website to work and that they want to scare people from going on the website when in fact we're hearing that security has been provided for.

CHAO:
I think that we've gone over and above because we are very sensitive and we appreciate the nerves (ph) that surround this new program with people's information.

TONKO:
Well, we appreciate you building the security of the website and for responding to the actions that's recommended in the ATO memo. Thank you so much. I yield back. MURPHY: Thank you. The gentleman's time has expired. Now, I recognize gentleman from Ohio, Mr. Johnson for five minutes.

JOHNSON:
Thank you Mr. Chairman. Mr. Chao I've spent 30 years in information technology. I've been the Chief Information Officer of publicly-traded companies as well as the Director of the CIO Staff at U.S. Special Operations

Command and I know the pressures that delivering on a system of this complexity. I know the pressures that are there. I assume that you and I have a common goal here today and that is to make sure that the American people hear the truth. Is that an accurate statement?

CHAO:
Correct.

JOHNSON:
OK. Given that then, would it be OK if you and I have an understanding because this is two IT guys talking to one another. If I ask you a question that you don't understand, would you ask me for clarifications so that we can get to the bottom of it because we want to dig down into your -- into some things that are pertinent.

CHAO:
Yes, sir.

JOHNSON:
OK, great. You know, under FISMA agencies, operating IT systems are required to establish security baselines, incorporate them into applications and networks and test them to see that they are incorporated correctly. The user review of this testing plan is typically known as a Security Control Assessment. Several of the security control assessments for healthcare.gov were either not completed or otherwise ignored. So are you familiar with the four security control assessments that were completed on the various aspects of the federally-facilitated marketplaces?

CHAO:
Not in intricate detail but I think -- going back to what you said about ignored or missed, I think the most important thing to remember is that on ...

JOHNSON:
Are you familiar with those security control assessments?

CHAO:
I ...

JOHNSON:
Have you seen or read them?

CHAO:
I've read the most important one, that's the one ...

JOHNSON:
Have you read all four of them?

CHAO:
No. Not all four.

JOHNSON:
OK. Could you turn to tab four of the document binder that you have in front of you. This is the Security Control Assessment completed on October 11th, 2013. Are you familiar with the findings of this security control assessment?

CHAO:
Yes.

JOHNSON:
OK. You testified a little earlier that that it was your opinion based on what you knew at the time that the security control assessments -- that security had been adequately addressed when Administrator Tavenner signed the document authorizing the operation of the website. Is that correct?

CHAO:
Yes.

JOHNSON:
But you just testified that you were not aware and you didn't read the security control assessments so how can you make that assertion that security had been adequately addressed when you hadn't even read the control assessment yourself?

CHAO:

I am thinking that there might be some mismatching versions here. Yours says final report October 11th for health insurance exchange August through September, 2013 SCA report. I have the federally-facilitated marketplace decision security report ...

JOHNSON:
Well, I'm talking about the one in your ...

(UNKNOWN)
Can we ask the witness to speak up a little bit. I'm having difficulties hearing you.

CHAO:
I'm sorry.

JOHNSON:
But I've got to move on because I don't have -- I don't have time to look through the binder. Who develops the scope of a security control assessment before the contractor performs it?

CHAO:
We have independent contractors that design our SCA testing.

JOHNSON:
Do you an application like the data services hub or the website to be complete in order to test it for purposes of a controlled -- security security control assessment.

CHAO:
I think that depends on -- you know we don't like testing security ...

JOHNSON:
Well I can assure that we don't.

CHAO:
The -- in terms of using live data, you know -- so prior that going to production, we tend to conduct security ...

JOHNSON:
Well, let me ask you a question. Let's put up a -- let's put up a slide, are you familiar with the term SQL injection? OK. You know SQL injection is a process that hackers use to gain access to SQL database -- relational (ph) databases through a SQL. This is a screenshot directly off of healthcare.gov that you see. If you put up -- if you put a semicolon (ph) in the search box, you get all of those different breakdowns of SQL injection. Can you give me any idea how vigorous the testing was around SQL injection and are you aware that, that users have -- potential hackers have the capability to go in through SQL injection and manipulate these strings.

CHAO:
I can't speak to the -- I can't speak to the exact -- that situation. I think some of the folks that are coming up behind me in the other panel might be able to specifically ...

JOHNSON:
I can assure you, Mr. Chairman that I still have very serious concerns about the security aspects of this system. With that, I yield back.

MURPHY:
Thank you. The gentleman's time has expired. Now, we recognize Ms. Schakowsky for five minutes.

SCHAKOWSKY:
All right. I want to also focus on this particular system that the contractor made. I'm here Mr. Chao, yes, OK. We've heard this morning, we just heard about the risks that the contract -- contractor, MITRE, identified when they performed security control assessments for different components of healthcare.gov. And at first glance, they can seem alarming. But my understanding is that all of these issues were mitigated for the functions on the website that launched on October 1st.

It's important to understand the general point of security testing to identify any potential - issues so they can be addressed before they become real problems. Asking neither to perform these assessments gave CMS and the contractors the opportunity to identify and resolve any security vulnerabilities before anyone's personal information could be put at risk.

So, Mr. Chao does that sound to you like an accurate description, do the security control assessments involve an iterative process where problem are identified and then mitigated.

CHAO:
Yes, that's correctly characterized.

SCHAKOWSKY:
So Mr. Chao, I want to walk through some of these keys security assessments to determine whether the high risks that MITRE identified we have in fact been addressed.

In January and February of 2013, MITRE of performed a security control assessment of EIDM (ph), the account creation function and healthcare.gov. According to the final report, MITRE identified several high risk findings. So Mr. Chao, were these high risks findings resolved and mitigated before the October 1st start of open enrollment in the federal market place.

CHAO:
Yes, they were.

SCHAKOWSKY:
And, the fact is that they were noted in the -- the backpack (ph) is noted in the MITRE report. OK, so MITRE also performed the security control assessment of the data services hub in August, 2013. And again -- and again, identified several high risk findings. We're these findings result and also mitigated before the actual for first launch.

CHAO:
Yes, and the hub received an authority to operate in August.

SCHAKOWSKY:
Yes and the fact is that was -- and that fact was noted in the report. I also want to discuss the security control assessment that MITRE performed over August and September, 2013 for the heath insurance exchange. Mr. Chao, we're all high risks identified in this assessment mitigated before October 1st?

CHAO:

Yes.

SCHAKOWSKY:
Thank you and what your answers confirm is that a system worked, neither identified potentially high risk -- high security risk. And CMS made sure that they we're mitigated before they would become major problem. The MITRE reports do not show a flood system, they show that CMS conducted security control assessment to identify problems. And then fix those problems and I hope that my Republican collegues will keep these findings in mind when they took about the security of healthcare.gov. We don't want to alarm the public about security risk and have a ready been addressed by CMS and in its contactors. It just seems to me that identifying risks that we're named. It's important also to note that they were all fixed before the launch on October 1st. And I thank you very much for your testimony, I yield back.

MURPHY:
Thank you. The gentle lady yields back, now we recognize the gentle lady from North Carolina, Mr. Ellmers for five minutes.

ELLMERS:
Thank you, Mr. Chairman and thank you Mr. Chao for being with us today. Mr. Chao I've a question about the subsidies some questions about on these calculation that could be happening on the exchange. Press reports have indicated that some subsidies are being miscalculated. In fact, one individual, the President identified that would beneficiary of Obamacare now can't afford it.

And Mr. Chairman, I'd ask unanimous consent to submit in article from CNN to the Committee for the report -- for the record. OK. This is a single mom who has a teenage son with ADHD. Went on the Washington State Exchange, had gotten a insurance quote for what she would pay at a gold (ph) price. Then she received notification that it was actually, the quote was actually higher for a silver plan, more confusion went on. Then even a cheaper plan at bronze level for $324. So, in other words, she ended up paying a lot more. I guess my questioning for you is, you know, is this happening on the healthcare.gov site or the federal market place?

CHAO:
I think there are a lot of inputs to how an advanced premium tax credit is calculated. The person can come back in make some modifications to their income levels, to their house of composition. So -- and Washington is a

(inaudible) base marketplace so I ca't really speak for that particular case. But I think healthcare.gov allows people the flexibility to try several ways to determine, you know, what there text credit.

ELLMERS:
OK, you know, and there again. I'm just going base of the article, it doesn't seems to be that she had gone back to make any changes. It sounded to me like, you know, there were miscalculations that she was notified up. So, again my questioning is, is this happening in the federal exchange?

CHAO:
I would need some specifics to be able to answer that. I think that if anyone ever done to have issues with believing that there subsidies were incorrectly calculated, they could certainly call center to try to find out if that was correct or not.

ELLMERS:
So that -- that's basically -- you know, I'm just asking how someone would address that or how that would happen if there were miscalculations, then you could speak to someone personally and ...

CHAO:
Yes. We have both a call center and what we call eligibility support workers.

ELLMERS:
Do you know if this is what's happening?

CHAO:
I'd ...

ELLMERS:
Have you heard any reports of ...

CHAO:
I think there are many calls from the call center for many different reasons. I don't know exactly, you know, I can't tell you there were 10 cases today or -- but ...

ELLMERS:
Did you know -- we can move on. I appreciate that. CGI, the contractor responsible for building healthcare.gov, can you explain your role with them in the last weeks of September. Did you, you know, were you in contact with them? Were you working with them one on one? Did you -- were you in their office?

CHAO:
Yes, I actually -- I moved down to (inaudible) and live in the hotel since September 10th to about the last week of October and I worked at CGI almost everyday.

ELLMERS:
So you were actually there in their offices working out of their office?

CHAO:
Yes.

ELLMERS:
One of the things that have -- I've got about a minute left on my time. The President announced the tech surge to fix the website, who's involve in these surge?

CHAO:
Their -- Todd Park is involve. And there are two fellows, one by the name of Mikey Dickeron, and another by the name of Greg Gershman.

ELLMERS:
Do you know about their compensation? How are they being compensated?

CHAO:
I have no insight to that.

ELLMERS:
Do they have a contract or did they have to sign an agreement?

CHAO:
I don't know.

ELLMERS:
Who were - who do these individuals report to?

CHAO:
I'm not -- actually I'm not sure who they have a contract with or whether they ...

ELLMERS:
So -- but you are in charge of the technical components you healthcare.gov? And they don't report to you?

CHAO:
No. They're part of a tech surge team that's being lead by Jeff Zients.

ELLMERS:
OK. So, Jeff Zeints in really the person that they are reporting to?

CHAO:
Right.

ELLMERS:
OK. Thank you very much. Mr. Chairman, my time has expired.

MURPHY:
The gentle lady yields back, we now go to Mr. Olson for 5 minutes.

OLSON:
I thank the Chair, and welcome Mr. Chao.

As you can imagine, sir, folks back home in Texas 22 have one simple question. Why -- why did healthcare.gov to come about -- .gov -- on October 1st with most people and (inaudible) yourself in every contract, you're writing the cost (ph) and do the testing and said, "Stop. Stop, stop, stop. We need more time." This Red Team document is frightening. Three or page 4 of the document, turns like limit end to end testing, parallel stacking of all phases. Stacking is vertical, not parallel. It's just time and scope of end to end testing launched at full volume. And previous 76TD e-mails, which you said you were worried that "crash the plane take off".

With all due respect sir, it never got to the runways. It was still waiting at the rafter (ph), waiting for the pilot, the bags, the fuel, waiting for new tires. Using the analogy and my records in naval aviator, healthcare.gov was a "hanger queen." Never ready to fly. I do want to talk about -- the folks back home I worked for are most concerned about protection of that personal health information.

We saw no testing that's concerned about the lack of Security Control Assessments, SCAs. And my question refers to -- free to the document brief there and on -- please turn to tab two, sir. My questions concerns, you guys said that this is the document you wrote for Ms. Tavenner, that you need a two part mitigation plan.

In part two is -- you said one of recommended steps is to "conduct a full SCA test on the FFM in a stable environment where all security controls can be tested within 60 to 90 days of going live October first." The FFM will not be completed by November 30th. So how is that the full test of the SCA within 60 days (inaudible)? How could that happen when you're losing 30 days off of that?

CHAO:
I think the 60 and 90 days refers to the inclusion of the final piece that needs to be built. What we mentioned earlier which I just want to says that it's actually 30 percent of the systems are left to be developed, and not 70 percent. And that 30 percent represents the payment aspect and the accounting aspects of making payments in the market place for all market places, not just the for fairly facilitated market places. And that functionality has to be in place for the January 1st effective date enrollments. And, so I think once we have that completed, we could do a full SCA across our entire system.

OLSON:
But sir, the document says October 1st roll out, 69 days after that. And apparently, right now, we're going to back to at least November 1st at the earliest for the roll out. I don't see how you -- 60 days or 90 days of testing before we go live again. One further question about the SCAs, how many SCAs did you identify and fixed before October 1st. How many have been identified since after roll out and how many are still out there? What's scope that my concessionaires (ph) should be worried about?

CHAO:

The most important aspect is that there or no high findings in the SCA test as of the October first roll out. And as I mentioned earlier, I read off a list of mitigation activities that we go over and above any system that we put in and deploy. We deploy and put in operations and monitor on the daily basis.

OLSON:
When can be, sir, that a full SCA will be conducted, system-wide?

CHAO:
When the last pieces of the system are completely built, which is not -- I don't want people to think that there hasn't been a full SCA. Full SCA has been conducted on the pieces that were needed for October 1st for eligibility enrolment. We have yet -- we still have to build the financial management aspects of the system which includes our accounting system and payment system and reconciliation system. Those will also have security testing involve as well.

OLSON:
And the full interim passing (ph), the whole full system, will we expect that to occur sir? What date?

CHAO:
I don't have an exact date but it should be in some time in December.

OLSON:
So 2013, not 2014, 2015, 2016?

CHAO:
Correct?

OLSON:
2013, OK sir. One final question. I want to refer back to your e-mail from July 16th about needing to feel more confident about the healthcare.gov. I'm assuming that some time in the last four months, you got that confidence. What gave that confidence? What was the trigger mechanism? When did that happens? Something has change last four months

CHAO:

I didn't say anything about having more confidence. I'm always cautious, which is what I was trying to say earlier is that, that until this is fixed until the vast majority of people who are having good experience going to through here, and we have people who want to enroll, get enrolled, particularly for January 1st, I'm going to continue to focus on that along with the rest of the team.

And, you know, so it's not really about confidence at all right now. It's about focusing on fixing the problem.

OLSON:
And so we're not buying that the "hanger queen" is still at the hanger. I yield back the balance of my time.

MURPHY:
The gentleman have yield back. What we're going to do is give each side five more total minutes just to get us a couple of clarifying questions. I have a couple of clarifying questions, if anybody from my side needs some time, we'll do that real quick. Ms. Degette.

DEGETTE:
Thank you, Mr. Chairman. Mr. Chao, I want o thank you for coming and spending the morning with us. I'm going to try to be quick because I'd like you to get back to wherever you're going to make this thing work, OK. The first thing I want to clear up because even though I thought we established it, the -- my friends on the other side continued to ask you about this McKinsey document at tab one. But I just wanted to clarify, you didn't -- you weren't part of this Red Team evaluation is that right?

CHAO:
Correct.

DEGETTE:
And you didn't really see this document until today, is that correct?

CHAO:
Correct.

DEGETTE:

So there were a lot of questions people ask you -- hypothetical questions people ask you about this evaluation that you really don't know the answer to because you weren't involve in the process and you didn't see the documents until today, right?

CHAO:
Correct.

DEGETTE:
Now, as I understand it, this evaluation was done in March, April 2013, is that your understanding as well of this McKinsey evaluation?

CHAO:
It's approximately at that time.

DEGETTE:
And do you have any knowledge of what that evaluation was supposed to be for? Was that a snapshot in time or do you even know?

CHAO:
From the interviews that I had with McKinsey, it was about really two things. One was I spent some time helping McKinsey understand the program. I mean, how it works, where we were in terms of status and schedule. I don't -- I suppose it's also includes a point in time kind of assessment because I educated them on exactly what was happening up to the date ...

DEGETTE:
Up to that time. Now on page four of these assessment, I don't really want you to respond to this because you weren't involve in the document, but I do want to point out, there were lot of questions that were asked today about the current situation involving requirements, multiple definitions of success, everything cetera. But the people who were asking those questions today didn't talk about the last thing which is in bold letters in a box that says, "CMS has been working to mitigate challenges resulting from program characteristics." This was in March or April.

And so without talking about this document necessarily but I think what your testimony -- what your job is really to identify issues throughout and try to mitigate them is that right?

CHAO:
Correct.

DEGETTE:
And that's what you've tried to do throughout.

CHAO:
It is a constant mitigation set of activities.

DEGETTE:
And the administration has said, "Let's going to try have the federal exchange site working for 80 percent of the people by the end of November." Is that right? That's what we've been reading in the press.

CHAO:
That's what the press quoted, I think ...

DEGETTE:
OK.

CHAO:
... what we've been saying is the vast majority of ...

DEGETTE:
All right. And do you believe that that's a reasonable goal at this point?

CHAO:
I think that's an obtainable goal given what I've seen so far.

DEGETTE:
Do you think it's going to happen?

CHAO:
I don't think there's any guarantees. I think we're still in a stage where we're trying to apply as much too diligence acquiring additional assistance, the tech surge looking at performance, fixing the functional defects along with

making sure that security monitoring is an on going basis. So I think there's still a lot of moving parts that it wouldn't be prudent to give 100 percent guarantees about where we going to be at on the exact ...

DEGETTE:
Well ...

CHAO:
... but I think we're on the right track.

DEGETTE:
OK, but what I would say to you is truly -- and you hear this from all of us. All of us were disappointed that it didn't work on October 1st. I'm sure you were, too.

CHAO:
Very.

DEGETTE:
And, so we need this to be essentially working, ASAP. For one thing, people who want insurance coverage as of January 1st have to sign up by December 15. So if it's not working for the vast majority of people by the end of November, that's going to hard to do. Understood?

CHAO:
We certainly understand that.

DEGETTE:
OK, one last thing, someone had asked you the question or had made the assertion that 60 percent of the site was not working. But I'm told that's not really accurate, that is really about 30 percent that's not working. And most of that is the back end which is the payment to insurance company, so that's not necessary the part that has to be working at this working at this moment. Is that correct?

CHAO:
It's not that it's not working, it's still being developed and tested.

DEGETTE:
OK, but that's the payment to the insurance companies, right?

CHAO:
Correct, which involves testing with charge fee and others.

DEGETTE:
All right, thanks, Mr. Chairman.

MURPHY:
Thank you. I recognize for five minutes. Just let me follow up here that and what you're saying there's 30 percent is yet to develop on the payment end. On October 1, the day this went live, how much of the site was developed at that time?

CHAO:
Probably, well 100 percent of all the priorities that we set for by the business for October 1st, it was up and running.

MURPHY:
OK, but what about the other parts?

CHAO:
I think there was a reprioritization associated with like shop employer, shop employee and the Spanish website that was ...

MURPHY:
But it was crashing for everybody. We've heard that it wasn't designed for that many people. It didn't pass the stress test. It never had end to end testing and you're saying it was 100 percent ready?

CHAO:
No.

MURPHY:
I just want to make sure we understand. What ...

CHAO:
It was 100 percent built.

MURPHY:
I understand built but just not working.

CHAO:
Yes, working functionally and ...

MURPHY:
Well then it's not built. If a car is built but you can't run the car, that car is not built. The website isn't working, it's not built.

CHAO:
Oh, I'm certainly not going to sit here and try to tell you that it was working well, so ...

MURPHY:
But you said on October 1, it was 100 percent built. I really need to know, because you had said before, you wish you had had more time. And you would -- just said to Ms Degette that your job was to identify issues and mitigate them, all right. And so there - and since you would have like to have more time and your job was to mitigate them, would you've like to seen this whole report from McKinsey that identify the problems so you didn't have to find them out?

CHAO:
Actually, I don't think it was necessary because I think this report was for really for Marilyn Tavenner and others. And that was written for that level of consumption in that audience.

MURPHY:
But you haven't seen it so you don't know. Or do you know.

CHAO:
I'm just assuming that - that's why I was -

MURPHY:

OK. I just want you to stick with the facts you know. So, well, what I'm seeing here is from March on, Mary Ann Bowen (ph), Jim Kurt (ph), Todd Park, Brian Steveck (ph), Michelle Snyder (Ph), Gary Cohen (ph), Bill Core (ph), Mike Hash (ph), Ariana Kalid (ph), Todd Park, Kathleen Sebelius, William Schultz (ph), Michelle Snyder (ph), Brian Steveck (ph), Marilyn Tavenner, Mark Shodas (ph), Jeanne Lambrew and Ellen Months (ph), all had briefings on this. Are those -- any people you work with?

CHAO:
I've been in meetings with several of those.

MURPHY:
Several of them since March and April?

CHAO:
Yes.

MURPHY:
And none of them raised any of these concerns to you who -- and you identify yourself is your job is to identify issues and mitigate them. But none of them identified that with all these interviews and the 200 documents reviewed, that there were these problems.

CHAO:
Within my day to day operational, you know, requirements to manage to contract to -- I mean to schedule to manage staffing.

MURPHY:
Yes, but what you don't measure, you can't win. And so I'm concerned that this list of people who you work with were not communicating to you. This document that you knew something existed because you indeed were interviewed on it yourself, yet here we have this messy roll out that didn't work. It crashed and only six people sign up the first day. And so our concern of our problems and yet it's puzzling to me why this key people just didn't talk to you about it?

Do you have any -- they gave you no hints that this existed?

CHAO:

Perhaps, that I just was not included in certain discussions.

MURPHY:
Well, if you knew then what you know now, would you have spoken up more with regards to rolling out this website in October 1?

CHAO:
I wish I had the luxury of a time machine to go back and change things but I can't do ...

MURPHY:
I understand that, but it is a matter that did you ask someone at that time for more time?

CHAO:
No.

MURPHY:
Why not?

CHAO:
Because my direction ...

MURPHY:
From?

CHAO:
... was to -- from Marilyn Tavenner is to deliver a system on October 1st.

MURPHY:
So, Marilyn Tavenner is to deliver October 1. She had been in on these briefings for McKinsey that said there were serious problems within at least, two of them I believe. And this was at HHS headquarters in April 4. She was there and also at the Eisenhower Executive Office building in April 6th. She was there, she's briefing these problems, she said move it for October 1 and you will submit, who is in charge to make sure this works. She didn't tell you that those problems existed? Is that what you're saying today?

CHAO:
I can't comment on that. I'd ...

MURPHY:
What's -- if she'd told you or she didn't tell you? I'm just curious.

CHAO:
I don't think she told me in the context of this briefing, no -- I think we have status meetings all the time in which we talk about ways to mitigate. And she ...

MURPHY:
You've seen here frequently over those months which she never brought up the extent of these concerns?

CHAO:
Not the McKinsey report, no. I think we've talked about certainly about issues and priorities for October 1st.

MURPHY:
I see. Well, I have no further questions, so Mr. Chao, I appreciate you spending so much time with us today. We're going to take a real quick five-minute break. We'll recognize our next panel of witnesses has been sitting here for a while.

So we'll be right back in five-minutes and thank you again, Mr. Chao.

CHAO:
Thank you.

(RECESS)

MURPHY:
All right this hearing is reconvened. I would now like to introduce the witness as in the second panel for today's hearing and thank you all for being so patient and waiting. Our first witness is Jason Providakes. He is the Senior Vice President and General Manager for the Center for Connected Government at MITRE Corporation. He is also the Director of the Centers for Medicare and Medicaid Services Alliance to modernize Medicare.

Our second witness is Maggie Bauer. She is the Senior Vice President of Health Services at Creative Computing Solutions, Inc, also known as CCSi. She has extensive operations and management experience in consulting, program management, IT infrastructure services, software development, life cycle and end user support on service local drive performance-based programs.

And our third witness is David Amsler. He is the Founder, President and Chief Information Officer at Foreground Security, Inc. He has more than 15 years or IT security experience. And he oversees the overall customer centric vision and direction of Foreground Security, its industry leading, offerings and day to day operations.

I'm now swearing the witnesses that you're all aware that the Committee is holding an investigative hearing? And when doing so, as a practice of taking testimony under oath, do you have any objections to testifying under oath?

BAUER:
No.

MURPHY:
All the witnesses are in negative there. The Chairman advice you that under the rules of the House and the rules to the Committee, you are intelligibly advised by council to anyone of you desired to be advised by a council during your testimony today. And all the witnesses just said no, in that case, would you please rise, raise your right hand and I'll swore you in.

You swear the testimony you are about to give is the truth, the whole truth and nothing but the truth?

And all the witnesses responded, I do. You're under oath and subject to the penalties set forth in Title 18, Section 1001 of the United States code. You may now give a five minute opening summary of your statement, Mr. Providakes.

PROVIDAKES:
All right. Well good morning Chairman Murphy and Ranking Member Degette. My name is Jason Providakes and I am here today on behalf of The MITRE Corporation. I serve as the director of the not for profit Federally Funded Research and Development Center, operated by MITRE and sponsored by the U.S. Department of Health and Human Services.

The MITRE Corporation is chartered in the public interest to apply systems engineering skills and advanced technology to address issues of critical and national importance. We accomplish this through the operation of research and development centers that support our government sponsors with scientific research and development, analysis, and systems engineering and integration as well. Known as Federally Funded Research and Development Centers, they are operated under a set of rules and constraints prescribed by the Federal Acquisition Regulations. The rules are designed to preserve the FFRDC's objectivity, independence and freedom from conflict of interest.

MITRE operates FFRDC centers for seven federal agency sponsors. We were awarded the contract to operate the CMS Alliance to Modernize Healthcare Center about a year ago, following a competitive bid. The center is charged with assisting CMS in modernizing its operations and supporting the implementation of health reform and expansion of health care to millions of Americans.

MITRE serves as a technical independent, objective advisor to CMS. We've been supporting CMS successfully since about 2005 on a contract basis prior to the establishment of the new center. We advise on Health IT, help plan and develop future policies, we provide technical evaluations and objective evaluation of business models, and assess new technology.

As part of its efforts to establish healthcare.gov, CMS asked MITRE to conduct security assessments on parts of the site. And I appreciate this opportunity to clarify what our role was in assisting CMS on healthcare.gov. We provide CMS with information security support and guidance under two contracts, the Office of Information Systems and Enterprise Information Systems Group. Pursuing to task issued under those contracts, MITRE performed a total of 18 Security Control Assessments, or SCAs, for components across a range of CMS enterprise systems. Most of these were performed on supporting infrastructure and development components. Six of the SCAs were directly related to healthcare.gov and were performed between September 2012 and September of 2013.

MITRE performs various tasks as part of overall support for CMS enterprise security maintenance. A limited amount of that support is in the form of external penetration testing relative to CMS websites including healthcare.gov.

MITRE is not in charge of security for healthcare.gov. We were not asked, nor did we perform end to end security testing. We have no view on the overall safety or security status of healthcare.gov.

MITRE did not and does not recommend approval or disapproval of an Authority to Operate. Deciding whether and when to grant an ATO is inherently a governmental function that derives from the government's assessment of overall risk posture. In this case, the government made its ATO decisions based on a large set of inputs and factors, among which were six SCAs performed by MITRE. We do not have visibility into the many other factors that went into the government's ATO decision. CMS did not advise MITRE whether or when ATOs were granted for the marketplace components being tested. In this case, the government made its ATO decisions based on a large set of data.

Again, we were not asked to conduct end to end testing, rather, we test specific parts of healthcare.gov under a set of specific parameters established by CMS. We worked alongside the CMS-designated contractor in the course of testing to remediate risks as high, and in almost all cases we succeeded. Our testing was accomplished in accordance with standard SCA engineering methodologies. In each case, we assessed component security control risks against CMS-defined security control parameters on a high, moderate, low scale, and we recommended appropriate risk mitigations.

On-site Security Control Assessment testing typically begins on a Monday and wraps up within a week. It tests against CMS-defined security control parameters. Over the course of the five days of testing, MITRE identifies the risks and assigns a remediation priorities for risks judged to be high and moderate levels.

Security testing is designed to flush out and pinpoint the security weaknesses of a digital information system. This enables corrective remediations to be applied and also allows the system operator to make the necessary business judgments and tradeoffs about the overall system. Because our role in performing the security control tests was limited in both time and scope, MITRE has no insight into how assessed security control risks were handled or what other risks may have surfaced subsequent to the date of testing. Judgments about the potential impact of assessed security control risks on overall system operations or performance were business judgments made by CMS as part of the operating authority.

Through our broader partnership with the federal government, we remain committed to assisting CMS in working to enhance the care and delivery of healthcare for all Americans. I would be happy to respond to your questions. Thank you.

MURPHY:

We now turn to Ms. Bauer for her opening statement.

BAUER:

Good afternoon, Chairman Murphy, Ranking Member Degette. My name is Maggie Bauer and I'm the Senior Vice President at Creative Computing Solutions, Inc, CCSi. I have a responsibility for CCSi's federal health contract including the Centers for Medicare and Medicaid Services, Veterans Affairs, the Department of Health and Human Services, National Institutes of Health and the Military Health Service. In addition to health-related services, CCSi delivers program and project management services, cyber security services, and enterprise systems engineering exclusively to the federal government. CCSi was founded in 1992 by Dr. Manju Bewtra.

In August of 2012, CMS awarded CCSi a contract to provide security oversight of the CMS eCloud. The eCloud refers to CMS's virtual data center which hosts systems and applications that support the Affordable Care Act. Foreground Security is our subcontractor on this contract and we function as a fully integrated team.

CCSi's role on this contract this to provide security operations monitoring and management including 24 by seven by 365 security monitoring from Secure Operation Center otherwise known as a SOC. We monitor the perimeter firewalls and network devices for the eCloud and we scan applications for security incidents.

These scans do not measure or track availability of downtimes or latency. If we detected anomaly, we follow the CMS-approved incident response plan procedures for identified security incidents such as network security configuration flaws or vulnerabilities in the network, security devices or in applications. CCSi's contract does not extend to remediating security incidents. CCSis' scope of work includes configuration, tuning, monitoring and management of CMS government-furnished equipment that reside in the Verizon Terremark security monitoring zone.

We review logged files, we conduct event analysis, we provide reporting on security incidents. All of these under the direction and supervision of CMS. Activities involving the development, scaling, testing, relief or administration of the federal exchange program, healthcare.gov, the federal exchange or the federally facilitated marketplace are not within the scope of our contract. I will be pleased to answer any questions that you have, thank you.

MURPHY:

Thank you, Ms. Bauer. And Mr. Amsler, you are recognized for five minutes.

AMSLER:

Thank you sir. Chairman Murphy, Ranking Member Degette, members of the Subcommittee, good afternoon and, and thank you for inviting me to testify at this hearing on the security of the website, healthcare.gov.

I am the President and Chief Information Offices of Foreground Security. I also founded the company. We provide cyber security consulting, training and services for both private sector and government agencies. Our clients include Fortune 100 companies, smaller but highly targeted firms and government agencies.

We defend our customer's against an increasingly intricate threat and threat actors through an integrated approach that entails building security architecture and assessing, monitoring and responding to attack against our customer environments.

Foreground Security is small but growing dedicated cyber security business located in Herndon, Virginia in Florida. Our roughly, 100 employees are highly-trained and committed to serving our clients.

Foreground Security is one of the company's hired to help develop a robust operational security management program for the new virtual data center created to implement the Affordable Care Act. We are subcontracted to our teammate, Creative Computing Solution Inc. or CCSi, which is the prime contractor for the Centers for Medicare and Medicaid services. Our role with CCSi includes a number of objectives relating to security environment of healthcare.gov.

I think of our role as encompassing three phases. First, is the creation of the security monitoring environment. This entails getting key staff in place, identifying needed security monitoring software and hardware, and building out a dedicated security operations center or SOC from which all monitoring is performed.

Second is building those security monitoring capabilities identified in phase one into the cloud environment itself. This has been the most challenging part of our contract in large part because we have had to construct security monitoring capabilities while the system itself is being built. Our work on this phase continues. And third, is actually monitoring the environment which itself can be thought of having two components. One is day to day, continuously searching for malicious activities including reporting and defending against them when they do occur.

The other is monitoring known, malicious actors or groups in advance of attacks to proactively identify the techniques or tactics they maybe using or planning to use to compromises environment. These are our main, end-state responsibilities relating to the security environments. We've worked very closely with CMS and Verizon Terremark on all phases of our work. CMS reviews and approves any capability we place in the environment and Verizon Terremark as the host of the environment, helps determine what security measures are placed in the virtual data center.

Perspective on our role is important. While our work for CMS is essential, it is narrowly focused and we are - were not involved in the design of the site, developing the software that runs it, or administration. To that end we do not monitor the site for performance purposes.

Foreground Security is just one member of the security team. In addition to the other companies represented today here on this panel, Verizon Terremark, URS, CGI and QSSI all play key roles in developing and testing the security of healthcare.gov.

I am proud of the work that Foreground Security has undertaken and continues to undertake in order to allow families and individuals looking for health insurance to use to healthcare.gov website, secure in their knowledge that their personal information is being protected which state of the art monitoring defenses. To this point, Foreground Security has filled it's obligations to CMS on time and under budget. We are dedicated to secure the operation at healthcare.gov and take extremely seriously our obligations to the public trust. I welcome any questions you may have.

MURPHY:
Thank you, Mr. Amsler. A couple of questions I want to begin with, first of all -- I'll start with you Mr. Amsler. Do you -- you were here for -- throughout Mr. Chao's testimonial, all three of you were. Do you have any concerns or any comments that was made by Mr. Chao?

AMSLER:
I wouldn't have any specific concerns.

MURPHY:
Ms. Bauer?

BAUER:
No.

MURPHY:
Mr. Providakes.

PROVIDAKES:
No concerns.

MURPHY:
All right. Mr. Amsler, you had said that in addition, (inaudible) companies represented today on this panel, Verizon Terremark, URS, CGI, and QSSI all played key roles in developing and testing to secure this healthcare.gov. Are you also referring to Ms. Bauer's company played a role in this?

AMSLER:
I view them as our teammate, I view them as one of us.

MURPHY:
But I thought in her testimony, she said that they were not then involve. So let me ask you, with this many companies involved, who did you whom reports to?

AMSLER:
Our customer was CMS and the security ...

MURPHY:
Is there a person?

AMSLER:
Our direct government technical lead, his name is Tom Shangquela (ph).

MURPHY:
And with regards to this, with all these companies involve that are playing key roles in developing and testing security, is that typical to have so many companies involved as oppose to one that's trying to do and work on this?

AMSLER:

Well, we've experienced all sizes of implementations. This one is obviously, certainly one of the largest that I've ever seen undertaken. I've certainly seen lots of people involve but probably not this many.

MURPHy: Mr. Providakes, is this typical to have so many companies involved in dealing with the security on the site?

PROVIDAKES:
Not really of number of companies are involved but getting two or three is not and typical to have on a complexity of a site like this.

Murphy: I just want that added to the complexity of trying to monitor security design.

PROVIDAKES:
If it's well-managed from a program perspective.

MURPHY:
Was it well-managed?

PROVIDAKES:
I would not know.

MURPHY:
From your perspective?

PROVIDAKES:
I don't -- we weren't involved in that level of insights but then I agree ...

MURPHY:
Ms. Bauer, we're you involve in that level and was well- managed from your point of view?

BAUER:
Our management from CMS has been known of very regular basis. We have daily meetings, in fact since healthcare.gov went live those meeting actually began or ramped up I should say to hourly and then backed away to every four hours and now they're on the shift basis at three times a day.

MURPHY:
You said activities involved in the development scaling, testing related to administration, the federal exchange program system, healthcare.gov, the federal exchange of the federally- facilitated marketplace or FFM are not within scope with your contracts. So you were not involved in the security issues involved with those websites?

BAUER:
The security, yes. But not the development scaling or testing of the healthcare.gov applications ...

MURPHY:
Were you involved the testing of the security?

BAUER:
Yes.

MURPHY:
And was it working?

BAUER:
Yes.

MURPHY:
At October 1?

BAUER:
Everything that was under our scope.

MURPHY:
Under your scope?

BAUER:
Yes.

MURPHY:

But in terms of how it relates to other parts, you don't know?

BAUER:
I would not allow ...

MURPHY:
OK. Mr. Amsler, how about for you? Were your parts working OK and your individual part and was that also touched (ph) with regards to the other?

AMSLER:
Congressman, to be clear for -- as far as work is concerned, our focus worked around operational monitoring security and some testing. We absolutely -- we're working. I can't speak to the rest of the groups and the teams that we're involved in development or even the SCA ...

(CROSSTALK)

MURPHY:
... typical, atypical and would you be concerned about how your parts work in conjunction with the site overall. Is that not the typical question that you would ask? I might -- it's like if you design a part for a car, you know your parts working. Would you like to know if the car works?

AMSLER:
Absolutely.

MURPHY:
And so that's I'm asking all of you. Would you like to know and then if your segments may have worked on their own but you did know what I worked in the whole system security, is that correct Mr. Providakes?

PROVIDAKES:
Well, that would be correct.

MURPHY:
Ms. Bauer?

BAUER:

Yes.

MURPHY:
OK. Mr. Providakes, CMS adopted the security control you develop, correct?

PROVIDAKES:
That's correct.

MURPHY:
And our -- these control are better than the applications at the direction of CMS.

PROVIDAKES:
They were assessed. Yes, they were embedded (inaudible) configuration changes where it may base on the configuration controls.

MURPHY:
And what point to the application development phase should security controls begin to be embedded into the application.

PROVIDAKES:
At the production phase. When we test -- generally when we test for the SCA, we're assuming that we are looking at the production-ready version of the application. And then we apply those CMS security controls we talked about and assess those against the production-ready version of that application.

MURPHY:
Are they embedded into the architecture healthcare.gov?

PROVIDAKES:
The overall CMS enterprise security controls are to be applied across all the systems of the healthcare.gov.

MURPHY:
They should be embedded in into healthcare.gov?

PROVIDAKES:
It should be.

MURPHY:
Were they?

PROVIDAKES:
I have no way of knowing that.

MURPHY:
Ms. Bauer, do you know if they were

BAUER:
I do not.

MURPHY:
Mr. Amsler?

AMSLER:
I wouldn't know the answer to that.

MURPHY:
OK. But you all worked in the security parts. You don't know if they were embedded and you don't know if anybody did touch (inaudible) seen it? Is that correct? Ms. Bauer?

BAUER:
Correct.

MURPHY:
Correct. Mr. Amsler?

AMSLER:
Correct.

MURPHY:

Thank you. And now we'll give -- I yield to Ms. Degette for five minutes.

DEGETTE:
Thank you, Mr. Chairman. As Mr. Chao testified, it's part of CMS's protocols that they hire independent contractors to test different parts of the security aspects of the site. Is that your understanding as well, Mr. Providakes

PROVIDAKES:
Yes it is.

DEGETTE:
And is it your Ms. Bauer? And is it yours Mr. Amsler?

AMSLER:
Yes.

DEGETTE:
So, Mr. Providakes, I want to ask you first, you testified your company was not hired to do the -- to perform end to end security testing. Is that correct?

PROVIDAKES:
That's correct.

DEGETTE:
And so what your job was to assess and identify risk and specific components of healthcare.gov to work with CMS and to address those concerns and report on the findings and results, is that correct?

PROVIDAKES:
That's correct.

DEGETTE:
And am I correct that in virtually all cases, when you did identify high risk in healthcare.gov components CMS was able to mitigate those risks before the system went live?

PROVIDAKES:

Yes, almost the high risks were mitigated.

DEGETTE:
And you said in your testimony, in your written testimony, MITRE is not in charge of security for healthcare.gov, we were not asked nor do we perform end to end security testing, we have no view of the overall safety or security status of healthcare.gov. That's because you were only asked to do a narrow assessment, a part of it, right?

PROVIDAKES:
A narrow assessment and scope in the time.

DEGETTE:
In time. Now, I just want to ask you, what's your personal view of the overall safety or security of healthcare.gov having worked on this at least some aspects of it?

PROVIDAKES:
Just my personal perspective, knowing CMS experience in the past as Henry Chao alluded to, they do a very solid job in terms of securing their systems historically.

DEGETTE:
And what you were doing was part of the same type things CMS has done to secure their systems in the past...

PROVIDAKES:
That's right.

DEGETTE:
Is that right?

PROVIDAKES:
That's correct.

DEGETTE:
Ms. Bauer -- as I understand it, Mr. Amsler, your company works sort of as a subcontractor of Ms. Bauer's company, is that right?

AMSLER:
Yes.

DEGETTE:
OK. So, what you folks to do is your company CSSi monitors the Firewalls and network devices for the Eclad (ph) that host healthcare.gov and scans the website application for security vulnerabilities, is that correct?

BAUER:
That's correct.

DEGETTE:
And on October 22nd, you briefed this Committee and I want to ask you, at that time had you detected any activity that you would consider to be out of the ordinary for a system like this?

BAUER:
Not out of the ordinary, no.

DEGETTE:
OK. And are you continuing to monitor the website moving forward?

BAUER:
Yes, we continue to perform all the functions of our contract.

DEGETTE:
And why is that?

BAUER:
I'm sorry?

DEGETTE:
Why are you continuing to monitor the function?

BAUER:
Because that's scope of our contract just continually monitoring.

DEGETTE:
OK. And have you detected any activity since October 22nd that you considered to be out of the ordinary?

BAUER:
We would detect the activity on a daily if not hourly basis. That's part of the nature of security monitoring, whether it's extreme or out of the ordinary, there's nothing that's been brought to my attention that would...

DEGETTE:
And would that be then reported to CMS?

BAUER:
Yes, there is an internet response plan and we follow the procedures of that plan.

DEGETTE:
And have you seen anything that would indicate some terrible problem with the website, vis a vis security?

BAUER:
Nothing that I have seen that's been escalated to me, no.

DEGETTE:
OK. And there's another contractor as I understand that's also been asked to look at other aspects, and that's (inaudible) and they're not here today, is that your understanding as well?

BAUER:
Yes.

DEGETTE:
So, is -- Ms. Bauer, has your company worked for CMS before and Mr. Providakes (inaudible) his task on security issues?

BAUER:
No, we have not.

DEGETTE:
OK.

BAUER:
But we do have other security work.

DEGETTE:
OK. And Mr. Amsler, what about your company?

AMSLER:
Not directly for CMS or HHS.

DEGETTE:
OK. So, you wouldn't know whether this kind of mirrors other security activity with CMS. But Mr. Providakes, you're telling me that what your company as done before, you're seeing a similar concern and readiness for security application?

PROVIDAKES:
Well, what I said was that following CMS's approach for security, they do execute, you know, 10, 20, 70 SCAs a year that we executed for CMS. So they're part of process, before they execute ATO they look for the input of this SCAs which is very rigorous process. The definition, defining a parameter the moment of time that we would conduct these SCAs for CMS as input to the ATO process.

DEGETTE:
OK. Thank you. Thanks, Mr. Chairman, I appreciate it.

MURPHY:
Let me ask clarifications on something Ms. Degette said. She asked her question about CMS and they're working as (inaudible) historically, were you referring then to the healthcare.gov website or in the past?

PROVIDAKES:
In the past broadly across CMS in terms of their security rigor that they apply across their systems.

MURPHY:
Thank you. Mr. Olson, you're recognized for five minutes.

OLSON:
I thank the Chair. And mostly want to thank the witnesses for your patience being here, it's been a long day. I know that -- very big (ph) questions I mean -- the Obamacare -- I'm sorry, healthcare.gov up and running is not rocket scientist. And that's good because if it were, we're simply waiting to land on the moon over 50 years later.

You may not have seen McKinsey report, the red team reported, have you all seen that.

BAUER:
I've not.

OLSON:
OK. You get copies too. I just want to ask some questions about report and apologize if you haven't seen it. But in comparison on page four, ideal large scale programs in the current states of healthcare.gov. And I wanted just some yes or no questions, do you agree with statements from this report. And (inaudible) comparing large scale ideal, large scale program development ideal program with characteristics of healthcare.gov.

The first obvious situation, clear articulation or requirements and discussed metrics. In healthcare.gov, have all the requirements an multiple definitions of success. Do you (inaudible) that's ideal and that's (inaudible) of healthcare.gov Mr. Providakes? Yes or no sir. So, (inaudible) to the spot.

PROVIDAKES:
It's really difficult to answer that question. Is that a apathetical question in terms of...

OLSON:
That's a yes (inaudible), this program is in clear articulation and it hasn't happened on healthcare.gov.

PROVIDAKES:

And that's where we would love to have clear articular requirements upfront, so you can design to, build to, test to, and that would be great, although it's rare, but would be great.

OLSON:
OK. And with all the requirements with healthcare.gov (inaudible) problem?

PROVIDAKES:
I'm not sure of the number (inaudible). I would think there were quite a number of requirements for healthcare.gov.

OLSON:
Ms. Bauer.

BAUER:
I would -- just having to consider (ph) briefly, I would...

OLSON:
I apologize (inaudible).

BAUER:
I would agree with the description of ideal, the ideal situation. However, I wouldn't have insight into the current situation because that' involves a development of healthcare.gov...

OLSON:
OK. Mr. Amsler.

Amsler: I would -- ideal is I agree with ideal. Again, we were involved in those aspects so I couldn't speak to it.

OLSON:
How about the program, their ideal is a sequential (ph) requirements designed (inaudible) testing and iteration revision between phases. And what the current situation is, parallel stacking of all phases. Do you agree Mr. Providakes? I apologize (inaudible)...

(CROSSTALK)

OLSON:
(Inaudible) your idealism. What...

PROVIDAKES:
It would create significant challenges to the program office to deliver that.

OLSON:
Has been parallel stacking?

PROVIDAKES:
It would be significant challenge to do that.

OLSON:
Ms. Bauer?

BAUER:
I would agree with that statement.

OLSON:
Mr. Amsler.

AMSLER:
Agree.

OLSON:
OK. How about in (inaudible) integrate operations and testing is the we all agree with that. And what happened is insufficient time and scope of end to end testing. Would you all agree with those statements? Yes or no.

PROVIDAKES:
And forgetting (inaudible) as you put it, you're saying, (inaudible) limited end to end testing. And in effect you have a hard date, I would (inaudible) that have limited time to do end to end testing. And these ones you could have done it (inaudible) there is limited time to do it.

OLSON:

Ms. Bauer.

BAUER:
Yeah. Generally I would agree I would have no insight building (ph) to what the increments were as regards to schedule. But, you know, you could create milestones and achieve ideally just about any goal if you create the milestones and achieve them on the way to the goal.

OLSON:
Mr. Amsler.

AMSLER:
End to end testing for me is pure security that's the world we live in and that's the world that we only live in. We can achieve a lot testing along the way but I will certainly -- I always shoot for ideal, ideal would be end to end testing.

OLSON:
And ideal a limited initial launch or a full launch not ideal. Last question, yes or now, do you agree with those statements? (Inaudible) it's not very good limited initial launch what we should be seeking (ph)?

PROVIDAKES:
A limited launch increases the risk obviously than a full, so increase risk.

OLSON:
Ms. Bauer?

BAUER:
I would actually suggest that perhaps this limited launch would have had a lower risk and then a full launch they have a larger risk whatever system you'd be deploying.

OLSON:
Mr. Amsler.

AMSLER:
I agree with Ms. Bauer's statement.

OLSON:
Well said, sir. One final question, I'm not trying to put you on the spot. (Inaudible) about how this program rolled out, are you comfortable putting yourselves and your families, putting personal information in healthcare.gov?

PROVIDAKES:
I have.

OLSON:
You're comfortable?

PROVIDAKES:
Yes. As a person who tries to (inaudible) on my case where knowing a limited amount of personal information I put up there and other information I feel comfortable personally but then (inaudible) apply to everyone.

OLSON:
Ms. Bauer, yes or no ma'am, comfortable?

BAUER:
Yes.

MURPHY:
Mr. Amsler.

AMSLER:
I'm actually very happy with my current healthcare.

OLSON:
Oh, boy, it's trying (inaudible) hornet (ph) says there. I yield back the balance of my time.

(CROSSTALK)

MURPHY:
Gentleman's time is expired. Ms. Degette, you have a clarifying question?

DEGETTE:
Thank you, Mr. Chairman. The questions that Mr. Olson was asking you folks were on this McKinsey document that we spent so much time with the last witness talking about tab one of the notebook. Have you seen that report before Mr. Providakes?

PROVIDAKES:
I'm familiar of this report.

DEGETTE:
OK. Ms. Bauer, have you seen it?

BAUER:
No I have not.

DEGETTE:
And Mr. Amsler, have you seen it?

AMSLER:
I have not.

DEGETTE:
OK. So, Mr. Providakes, the two of you, any then Ms. Bauer and Mr. Amsler, any answers you were giving were really just based on speculation since you weren't -- they haven't seen it or involved with it, is that right?

BAUER:
Yes.

DEGETTE:
Mr. Amsler?

AMSLER:
That's correct.

DEGETTE:

OK, Mr. Providakes. So Mr. Olson was asking you about some of this recommendation. This is from last spring, it was a snapshot in time on page four of that report. At the bottom where he was talking about evolving requirements and multiple definitions of success et cetera, that (inaudible) forgot to mention which was the part also I noticed they forgot to mention when the previous witness was a -- is the part that's in the box in bold type at the bottom of all of those current situation bullets, which says, "CMS has been working to mitigate challenges resulting from program characteristic." Do you see that?

PROVIDAKES:
I do see that.

DEGETTE:
What does that mean to you?

PROVIDAKES:
Well, it means, you know, they recognized the risk and the challenge of the program and they were looking at options or mitigation approaches that would minimize the risk.

DEGETTE:
So, CMS hired McKinsey to do an evaluation of the program and come up with some concerns that they could then work to mitigate, is that right?

PROVIDAKES:
Only what I -- yes.

DEGETTE:
And that's the same reason they hired your company to do security assessment is to find places where there might be problems and to make recommendations that they could then work to mitigate, is that right?

PROVIDAKES:
That's correct. Identify risk to mitigate risk.

DEGETTE:

And in your view, at least the recommendations your company made, did they in fact work to mitigate those risks?

PROVIDAKES:
In the context for the SCA, yes.

DEGETTE:
Thank you very much. Mr. Chairman, I have no further question.

MURPHY:
Have you seen this document today Mr. Providakes?

PROVIDAKES:
I'm familiar of the document. It's been a while.

MURPHY:
So you're familiar, so when they say they've been working to mitigate challenges, you are personally aware that some of these mitigations were taking place or you are just saying so today?

PROVIDAKES:
No, I have no idea of what mitigation -- whether (ph) they took the recommendation of this...

MURPHY:
I was curious because you're drawing conclusions but I didn't know if you (inaudible). So that's based upon yesterday.

PROVIDAKES:
Based upon?

MURPHY:
OK. So a quick thing, Mr. Amsler, while developing a security measures for the cloud environment, have you encountered any challenges at all?

AMSLER:

Certainly, lots of challenges along the way. Congressman, did you mean more implementing them or certain things?

MURPHY:
Sort of some things or if they're different from what you're used to hear or anything standing out to you that's a concern with regard to the cloud environment and the security there?

AMSLER:
Well, cloud in and out of itself brings a unique set of challenges that any of us in the industry are all trying to deal with.

MURPHY:
That's a system that you can't miss how to correct right now with the cloud environment. It's on its own, it's like secure concern.

AMSLER:
I agree, this is our biggest, one of our biggest challenges that we're facing as an industry today. That's in the (inaudible) security...

MURPHY:
Who's in charge of that cloud environment?

AMSLER:
Horizon, CareMark and I assume you mean actually owns it and controls it.

MURPHY:
And how difficult is it to develop these security measures while the system is being built?

AMSLER:
That would not be ideal.

MURPHY:
Do you have all the tools and capabilities now to successfully and fully monitor the system?

AMSLER:
I'm a unique animal in that. I've live, eat and breathe cyber security. And as a company, we do (inaudible) only strive for better. I'm always striving to make it the...

MURPHY:
Do you have all the tools now you need to fully monitor the system?

AMSLER:
We have a set of controls that exceed any standard set up control.

MURPHY:
I understand you're trying to do a great job, I appreciate that. I'm just trying to get a sense of -- have you been limited in anyway in your ability to do all the things you would like to do with your excellent team in place?

AMSLER:
There are some things that we have asked for that are not in placed as of yet.

MURPHY:
Such as what?

AMSLER:
These would -- they're very technical in nature. Again, we have a standard set up control. So we're only...

(UNKNOWN)
Mr. Chairman, we want to have (ph) and give us that information...

MURPHY:
Yes. Could you (inaudible) that?

(UNKNOWN)
I definitely would like to move (ph) private instead of public (inaudible)...

AMSLER:

I would be happy to get with my team and get...

MURPHY:
I appreciate that. Ms. Bauer, do you have all the tool necessary to fully?

BAUER:
(Inaudible) are potentially the same because we're an integrated team. I would agree with Dave.

MURPHY:
All right. And Mr. Providakes do you have all the tools necessary to fully do your work here?

PROVIDAKES:
Well, (inaudible) different role, but yes.

MURPHY:
I see. So let me ask this within regard to how things are. If the system -- have there been any attempts, you wonder what you've monitor Ms. Bauer and Mr. Amsler, any attempts of hack in the system that you can tell?

AMSLER:
Congressman, the simple answer is yes. The longer answer is I don't have an environment where it's not being attack today though.

MURPHY:
I understand. So we took (inaudible) is that is the system now, are you saying that it's fully secure from external hackers trying to get in?

AMSLER:
I've never -- we live in a world of not if but more when. That's the nature of the world we're live in today. So I can never give you again, see that that's someone is not going to get in. It's probably going to happen at some point, but we have designed it limit the damage and identify it as quick as possible.

MURPHY:
So we can at this point sign offs till the system as fully secure. It's an ongoing process you're saying...

AMSLER:
It's always ongoing process. Today I feel comfortable with the capabilities we have put in place, but I'm always striving for more.

MURPHY:
I understand, and Ms. Bauer, would you agree with that assessment?

BAUER:
I would David is answering your...

MURPHY:
You have to talk in your microphone (inaudible).

BAUER:
(inaudible) very technical (ph) perspective, but I would say that from our perspective with regard to the tools and appliances we have in place, right now today, the system is secure as David says, security is always evolving. It's always dynamic and ongoing and we're always going to want to do better and keep on top of the latest technology, the latest appliances. So we'll always be maturing. But as regards, the scope of our contract and the appliances and tools and practices we have in place, we are confident.

MURPHY:
And I appreciate you standards of excellence and I appreciate you understand this is an evolving process. But given the concern with security, what I'm hearing from you is nobody can really give 100 percent guarantee that this website is secure with the regards to the data that has the personally-identifiable information (inaudible) for those things and there no (inaudible) guarantee that some hacker is going to try and get into it and that they have -- they will continue to try and probe until they get through, is that what you're saying?

PROVIDAKES:
But I also would say the same thing about Facebook or any banking website as well...

MURPHY:
Sure.

PROVIDAKES:
... (inaudible) unfortunately the world we live in today.

MURPHY:
Appreciate that. Same for you Ms. Bauer?

BAUER:
Yes, and I think that the critical factor is the rigor with which have procedures in place to identify any risk, any vulnerabilities and then work to mitigate them. And we have very robust procedures in place for that.

MURPHY:
Very good.

All right, I appreciate the comments from the panel today and I ask unanimous consent that the written opening statements of other member we introduce into the record of this (inaudible). And without objection, those documents will be in the record.

I also ask unanimous consent that the contents of the documents (inaudible) to be introduced in the records to authorize that to make appropriate reductions.

And without objection, reductions will be entered for the record with any reduction the staff determines are appropriate. So, in conclusion, I'd like to thank all the witnesses and members that participated in today's hearing. I remind members they have 10 business days to submit questions for the record (inaudible) ask the witnesses to all please agree to answer appropriate to the questions and we will work out some mechanism to enter some in confidential in- camera (ph) discussions.

And with that, this hearing is concluded.

(UNKNOWN)
Thank you.

CQ Transcriptions, Nov. 19, 2013

List of Panel Members and Witnesses

PANEL MEMBERS:
REP. TIM MURPHY, R-PA. CHAIRMAN

REP. MICHAEL C. BURGESS, R-TEXAS

REP. MARSHA BLACKBURN, R-TENN.

REP. PHIL GINGREY, R-GA.

REP. STEVE SCALISE, R-LA.

REP. CORY GARDNER, R-COLO.

REP. MORGAN GRIFFITH, R-VA.

REP. GREGG HARPER, R-MISS.

REP. PETE OLSON, R-TEXAS

REP. RENEE ELLMERS, R-N.C.

REP. BILL JOHNSON, R-OHIO

REP. BILLY LONG, R-MO.

REP. JOE L. BARTON, R-TEXAS EX OFFICIO

REP. FRED UPTON, R-MICH. EX OFFICIO

REP. DIANA DEGETTE, D-COLO. RANKING MEMBER

REP. GENE GREEN, D-TEXAS

REP. JAN SCHAKOWSKY, D-ILL.

REP. KATHY CASTOR, D-FLA.

REP. BRUCE BRALEY, D-IOWA

REP. G.K. BUTTERFIELD, D-N.C.

REP. BEN RAY LUJAN, D-N.M.

REP. PAUL TONKO, D-N.Y.

REP. PETER WELCH, D-VT.

REP. JOHN D. DINGELL, D-MICH. EX OFFICIO

REP. HENRY A. WAXMAN, D-CALIF. EX OFFICIO

WITNESSES:

HENRY CHAO, DEPUTY CHIEF INFORMATION OFFICER, DEPUTY DIRECTOR, OFFICE OF INFORMATION SERVICES, CENTERS FOR MEDICARE AND MEDICAID SERVICES

DAVID AMSLER, PRESIDENT AND CIO, FOREGROUND SECURITY, INC.

MAGGIE BAUER, SENIOR VICE PRESIDENT, HEALTH SERVICES CREATIVE COMPUTING SOLUTIONS, INC.

JASON PROVIDAKES, SENIOR VICE PRESIDENT AND GENERAL MANAGER, CENTER FOR CONNECTED GOVERNMENT, MITRE CORPORATION

Source: **CQ Transcriptions**
© 2013 CQ Roll Call All Rights Reserved.

Exhibit 12

TurningPoint. Federal Marketplace Program System (FMPS) Independent Verification & Validation (IV&V) Assessment 6 Report. Apr. 19, 2013.

CENTERS FOR MEDICARE & MEDICAID SERVICES

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

Federal Exchange Program System (FEPS)

Independent Verification & Validation (IV&V) Assessment 6 Report (Testing Playbook)

Version 1.0

April 19, 2013

Prepared by:

TurningPoint
Turning Point Global Solutions
Software Services Company™

Document Number: FEPSIV&V-IAR-06-TP
Contract Number: HHSM-500-2012-00008U

CMS SENSITIVE INFORMATION—REQUIRES SPECIAL HANDLING

APPROVALS

Exchange IT Program Approving Authority:

Signature	Printed Name	Date	Phone Number

Monique Outerbridge, CMS/OIS/CIISG, Director

Signature	Printed Name	Date	Phone Number

Paul Donohoe, CMS/OIS/CIISG, Testing Coordinator, Forward Engineering Team

Signature	Printed Name	Date	Phone Number

Shawn Hunter, CMS/OIS/CIISG, Government Task Lead

REVISION HISTORY

Version	Date	Organization/Point of Contact	Description of Change
1.0	04/19/2013	TurningPoint	Initial submission

Table of Contents

EXECUTIVE SUMMARY 1

1 INTRODUCTION 1

1.1 BACKGROUND 1
1.2 SCOPE 1
1.3 FEPS OVERVIEW 1
1.4 IV&V APPROACH AND METHODS 1
1.5 ASSUMPTIONS 3
1.6 CONSTRAINTS 3
1.7 REFERENCES 3

2 FEPS TESTING PLAYBOOK 4

2.1 QUALITY ASSURANCE (QA) 4
2.2 OPERATING ENVIRONMENT 7
2.3 SYSTEM AND ACCEPTANCE TEST 9
2.4 OPERATIONS OVERSIGHT 20

APPENDICES 21

APPENDIX A: ACRONYMS 22

APPENDIX B: STAKEHOLDERS INTERVIEWED 23

APPENDIX C: DOCUMENTATION REVIEWED 24

APPENDIX D: RISK DETERMINATION 25

D.1 RISK DESCRIPTION 25
D.2 RISK DETERMINATION 25
D.3 RISK MITIGATION AND RECOMMENDATIONS 26

Figures

Figure 1: Findings by Scope of Service Area 1
Figure 2: Total Findings by Risk Level 2

Tables

Table 1: Findings by Area 1
Table 1-1: Findings Table Terminology 2
Table 1-2: Findings Categories 2
Table 2-1 Quality Assurance Findings 4
Table 2-2 Operating Environment Findings 7
Table 2-1 System and Acceptance Test Findings 9
Table 2-1 Operations Oversight Findings 20
Table B-1 Interviews & Meetings 23

Table C-1 Documentation Reviewed 24
Table D-1 Risk Scale and Necessary Actions 25
Table D-2 Probability Assessment Criteria 26
Table D-3 Impact Assessment Criteria 27
Table D-4 Risk Value 27

EXECUTIVE SUMMARY

This report presents the results of the third assessment by the Independent Verification & Validation (IV&V) contractor, TurningPoint Global Solutions, which was tasked by the Centers for Medicare and Medicaid Services (CMS) to provide quarterly technical audits of the Federal Exchange Program System (FEPS).

The FEPS Testing Playbook is an excellent strategic initiative to meet the business need to identify all major gate reviews, hand-offs, coordination points and organizational roles and responsibilities for supporting both internal and external testing activities.

Table 1: Findings by Area

Total Findings				
	Low	Moderate	High	Total
Quality Management		3	1	4
Operating Environment		3	1	4
System Acceptance Testing	3	11	4	18
Operations Oversight	1		1	2
Total	**4**	**17**	**7**	**28**

Figure 1 displays a summary of findings for this assessment, with a distribution of risk levels. A description of the determination of risk levels appears in Appendix D: Risk Determination.

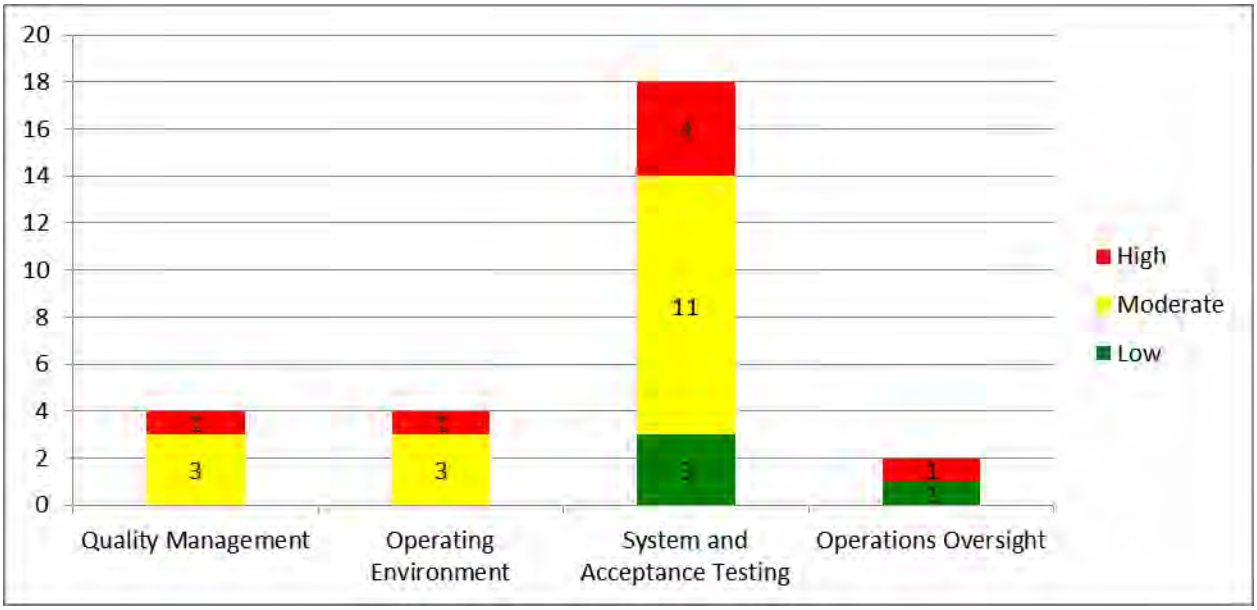


Figure 1: Findings by Scope of Service Area

Figure 2 displays a summary of total findings by risk level.

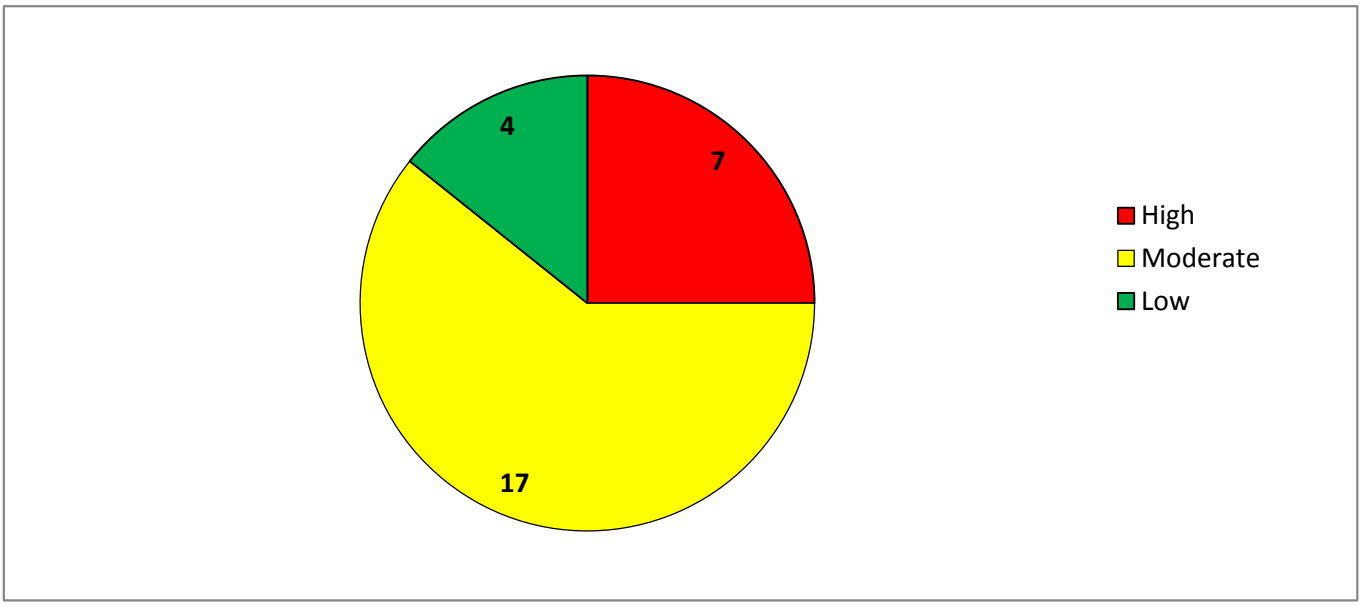


Figure 2: Total Findings by Risk Level

RECOMMENDATIONS

The IV&V team recommends the following:

1. The following recommendations are made for stage gate reviews:
   - Discussions about and implementation of the stage gate process should take place prior to the stage gate review.
   - Adhere to meeting agendas.
   - Conduct the review and determine if corrective actions are needed.
   - Verify corrective actions when appropriate.

2. CMS needs to mandate that the results of reviews on FEPS (including milestones and stage gate reviews) are published and signed-off on prior to the promotion of the accompanying code base to ensure that the delivered system satisfies the business needs.

3. An Environment usage schedule needs to be published, containing:
   - Who - the contractor(s) currently testing in each environment
   - What - the service(s) or testing windows for each service currently undergoing testing in each environment
   - Related code build deployment information
   - When – the scheduled timeframe for the anticipated testing cycle in each environment

- How - List constraints, dependencies, interdependencies, conflicts if when a particular service is being tested [i.e., when a unique service is being tested (Medicaid), the environment will not be available for testing]
- Scheduled outages.

4. Make the Testing "Playbook" into a "book"; Re-do the FEPS Testing Playbook into a Word document and re-arrange it in a more useful format to permit its purposeful use to:
   - Act as the primary source of CMS guidance when it comes to performing all testing processes, milestones/gate reviews, artifacts, and documents.
   - Act as a "living" document to identify all major gate reviews, hand-offs, coordination points and organizational roles and responsibilities for supporting both internal and external testing activities.
   - Design streamlined processes for the different stages and types of testing (Developer Unit, Internal, External, Performance Stress, End-to-End, and Production Readiness).

5. Include backup and restore procedures and guidelines in the Testing Playbook.

1 INTRODUCTION

1.1 BACKGROUND

The FEPS program was initiated by CMS to provide health insurance exchange capabilities required by the Patient Protection and Affordable Care Act (ACA) of 2010. In support of the FEPS effort, CMS employed TurningPoint to provide an independent and unbiased analysis of the FEPS components and artifacts. CMS tailored the IEEE 1012 standard to 106 V&V service areas covering the nine Scope of Service areas in the FEPS IV&V Statement of Work (SOW): Quality Management, Training, Requirements Management, Operating Environment, System And Acceptance Testing, Data Management, and Operations Oversight. Not all service areas will be covered in all assessments.

1.2 SCOPE

The scope of this assessment is the FEPS Testing Playbook v0 33 03 12 13.

1.3 FEPS OVERVIEW

The IV&V team analyzed and organized the assessment of the FEPS Testing Playbook under the following service areas:

- Quality Management
- Operating Environment
- System And Acceptance Testing
- Operations Oversight

1.4 IV&V APPROACH AND METHODS

For this assessment, our approach included: planning the scope of the assessment, identifying the documentation, and identifying the standards to use. The IV&V approach to working with federal and contractor organizations is cordial and supportive of priorities, while maintaining independence and objectivity during the assessment.

The IV&V team used CALT to identify the artifacts related to the scope of the assessment, and then used the IV&V service areas and the IV&V checklist. In addition the team used ITIL standards to evaluate the Testing Playbook.

The findings are only related to the Testing Playbook. Each finding includes an IEEE categorization, impact statement, sources, risk probability, risk impact, and risk value. See Appendix D: Risk Determination for more detailed information about the method used to determine risk impact, probability and value.

Table 1-1 below defines the terminology used in findings tables.

Table 1-1: Findings Table Terminology

Findings Table Heading	Description
Task Number	Pulled from FEPS IV&V SOW
Task Description	Pulled from FEPS IV&V SOW
Finding	Based on category description table below
Finding Description & Evidence	Results of IV&V evaluation
Source	List of information source used to make determinations
Recommendation	Results of IV&V evaluation

A Finding or Anomaly is anything observed in the documentation or operation of software that deviates from expectations based on previously verified software products or reference documents (IEEE 1012).

Table 1-2 below depicts the definition of finding categories used in the tables in this report.

Table 1-2: Findings Categories

Category	Description
Future Assessment	This area was not assessed by IV&V during this reporting period.
No "X" Activity Occurred	No project activity occurred in the area of "X" for the scope of this assessment.
Process Deviation	Documentation or practices indicate the project has deviated from the defined and approved policy, process or procedure.
Completeness	The state of being complete and entire; having all necessary parts, elements, or steps.
Correctness	(1) The degree to which a system or component is free from faults in its specification, design, and implementation. (2) The degree to which software, documentation, or other items meet specified requirements. (3) The degree to which software, documentation, or other items meet user needs and expectations, whether specified or not (Wikipedia).
Consistency	The degree of uniformity, standardization, and freedom from contradiction among the documents or parts of a system or component (IEEE 1012).
Accuracy	(1) A qualitative assessment of correctness, or freedom from error. (2) A quantitative measure of the magnitude of error. (IEEE 610.12-1990)
Readability	Readability is the ease in which text can be read and understood by people. The readability of a program is related to its maintainability, and is thus a critical factor in overall software quality.
Positive Finding	This area was assessed by IV&V and the following positive items are noted.
Verifiability	(1) The extent to which the evaluation of a system or component can be performed. (2) The extent to which the correctness of a system can be determined
Testability	(1) The degree to which a system or component facilitates the establishment of test criteria and the performance of tests to determine whether those criteria have been met. (2) The degree to which a requirement is stated in terms that permit establishment of test criteria and performance of tests to determine whether those criteria have been met (IEEE 610.12-1990).

Category	Description
Traceability	The ability to link product requirements back to stakeholders' rationales and forward to corresponding design artifacts, code, and test cases. Traceability supports numerous software engineering activities such as change impact analysis, compliance verification or trace back of code, regression test selection, and requirements validation. It is usually accomplished in the form of a matrix created for the verification and validation of the project.
No change	This area was assessed by IV&V and no change was found between this assessment and the previous one.
Process Improvements	This is an area that has no problems in correctness, completeness, consistency or accuracy. It is only an area identified for possible improvement.

1.5 ASSUMPTIONS

The IV&V team made the following assumptions during this assessment:

- The Testing Playbook in the CALT repository is version v0 33 03 12 13.
- Information derived from the Milestone and Stage Gate reviews held during the assessment may be included in the assessment.

1.6 CONSTRAINTS

The IV&V team was constrained by the following during this assessment:

- Due to time constraints, no interviews were conducted; this is only a review of the Testing Playbook presentation in CALT.

1.7 REFERENCES

The standards listed below were utilized for the IV&V team's review of the FEPS Program and in the preparation of this report.

- IEEE Standard for Software Verification and Validation 1012-2004
- The Software Engineering Institute (SEI) Capability Maturity Model Integration (CMMI)
- Project Management Institute's Project Management Body of Knowledge (PMBOK)
- CMS Expedited Lifecycle Process (XLC)
- Information Technology (IT) Infrastructure Library (ITIL) v3 standards

2 FEPS TESTING PLAYBOOK

This section covers detailed findings of the scope of services identified for review as specified in the FEPS IV&V Statement of Work. Each section will list areas of review, detailed findings, and supporting evidence.

2.1 QUALITY MANAGEMENT (QM)

Table 2-1 Quality Management Findings

IV&V Task: QA-1	**Verify QA organization monitors the fidelity of all defined processes in all phases of the project.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Verifiability:** For Internal & External Testing Activities, it is not clear whether a QA organization is monitoring the fidelity of defined test processes in all phases of the project.	3	3	9	**Moderate**
Finding Detail	QA is mentioned in the context of 'Design/Development/QA' (Slide 8, Internal Testing Activities Layout, Slide 18 Internal Testing – Milestone Activities Test Analysis (TA)); however, it is not clear whether a QA organization is monitoring the established processes and outputs from various testing activities and milestones to provide timely project feedback.				
Potential Impact	If a QA organization is not monitoring the fidelity of all defined processes in all phases of the FEPS project, then there is no assurance provided that the delivered system will have quality imbedded into the system lifecycle which may lead to unstable and unpredictable results in production.				
Recommendation	Empower the QA organization to be fully involved in the project lifecycle and request reports, audits, etc., to assure stakeholders that the developing system is adhering to the quality measures as stated in the FFE PMP and FFE QMP.				
Source(s)	**CALT:** doc23938 FEPS Testing Playbook doc4371 CMS Federal Facilitated Exchange Project Management Plan_v 1 0_02062012a doc4380 FFE Quality Management Plan_v1.0_Final Draft				
IV&V Task: QA-4	**Verify that the quality of all products produced by the project is monitored by formal reviews and sign-offs.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Correctness:** The Sprint 15 Document Readiness Review (DRR) did not follow the Testing Playbook.	5	2	10	**Moderate**

Finding Detail	The purpose of the meeting was stated as: Making sure the test artifacts, handoffs and milestones were well documented; and the documentation was captured in one location to be accessible by all stakeholders. However, the following items were discussed: • The checklist input and output identification schemes; the various multiple locations that the documents could be saved, finally settling on the use of CALT to version a 90% draft and final. • Mathematica needed to deliver data within 3 days of the DRR and the problems Mathematica was having in doing this because no one is informing them when the schema changes. • The sample data for legs 1 and 4 and why it could not be delivered for legs 2 and 3. • Slide 9, of the presentation, shows the FFE BSDs are inputs to the DRR when they are not ready. • User guides would not be at 90% complete by DRR. • Slide 10, of the presentation, is incorrect because Sprint 15 did not have any external services. • Who would own the schedule for tracking the development of test data. • Who understands the schedule of the environments and could a schedule be provided and distributed; and there needed to be a link to the Hub service forecast so that everyone could understand what was coming up. Though these topics may have needed discussion, they were not part of the agenda and Sprint 15 document quality was not discussed, and the location of the documents was not verified. This was not a formal review and there were no sign-offs or decisions made.				
Potential Impact	If meetings do not follow the Testing Playbook, then milestone activities and processes may not be completed and the meeting may not address all the critical issues.				
Recommendation	The following recommendations are made for Stage Gate reviews: • Discussions about and implementation of the process should take place prior to the Stage Gate review. • Adhere to meeting agendas. • Conduct the review and determine if corrective actions are needed. • Verify corrective actions when appropriate.				
Source(s)	**CALT:** doc23938 FEPS Testing Playbook **Meeting:** DRR on 3/25/2013				
IV&V Task: QA-4	**Verify that the quality of all products produced by the project is monitored by formal reviews and sign-offs.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 2	**Correctness:** The Release 5 Test Execution Review (TEX) did not follow the Testing Playbook.	3	4	12	**Moderate**
Finding Detail	The meeting discussion and presentation did not include the primary input, TEX Checklist, identified in Slide 7 of the meeting presentation. This should be presented at the start of the meeting along with a notification to participants regarding the success criteria for the TEX. The meeting conclusion was open-ended without resolution of expected outputs.				

Potential Impact	If the TEX leaves items unresolved to be discussed at a future meeting, then the TEX milestone is not met and this may have an impact to availability of the production release.				
Recommendation	The following recommendations are made for Stage Gate reviews: • Discussions about and implementation of the process should take place prior to the Stage Gate review. • Inputs should be clearly identified as complete at the start of the meeting. • Outputs reviewed and determined if deficient or ready to proceed • Success criteria should include formal agreement to proceed				
Source(s)	**CALT:** doc23938 FEPS Testing Playbook **Meeting:** Release 5 TEX on 4/16/2013				
QA-4		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 3	**Consistency:** It is not apparent whether adverse quality reviews and their outcomes impact the promotion of delivered code.	**4**	**4**	**16**	**High**
Finding Detail	For Internal (Slide 16) & External Testing Activities (Slide 30), it is not clear what the acceptance criterion are, and if an adverse quality review negatively affects the promotion of the delivered code base (i.e., are the business products delivered at each Stage Gate reviews fit for their intended use and meets the business need?). For example, a Validation Readiness Review (VRR) is performed prior to the start of Validation Testing and includes System Testing, Functional Testing, End-to-End (E2E) Integration Testing, Regression Testing, and Section 508 Testing; however, no conditional paths are depicted if any of the test activities. • Slide 83, Sprint Internal Validation/Release Internal Validation; • Slide 87, Formal – External Test Types • Slide 92, the VRR for E2E Testing – All Partners • Slide 93, Production Readiness (PR) The FFE QMP (pg.3) states "…the QM approach must ensure that the business product delivered is fit for its intended use and meets the business need…"				
Potential Impact	If the results of Stage Gate reviews do not have an impact on the promotion of the delivered code base then the business products delivered at each Stage Gate reviews may not be fit for their intended use, will not meet the business need and will increase overall project costs through re-work downstream and further into the project lifecycle.				
Recommendation	CMS needs to mandate that the results of quality reviews on FEPS (including milestones and Stage Gate reviews) are published and signed-off on prior to the promotion of the accompanying code base to ensure that the delivered system satisfies the business needs.				
Source(s)	**CALT:** doc23938 FEPS Testing Playbook				

2.2 OPERATING ENVIRONMENT

Table 2-2 Operating Environment Findings

IV&V Task: OE-1	**Evaluate new and existing system hardware configurations to determine if their performance is adequate to meet existing and proposed system requirements.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Completeness:** Readiness of the environments for testing is not included in the Stage Gate review as inputs.	**4**	**3**	**12**	**Moderate**
Finding Detail	Identification of the next stage environment and its readiness is required for moving forward to the next stage in the Life Cycle Process.				
Potential Impact	If the information is not available, then a decision to move forward to the next stage may be made without an available environment causing schedule delays.				
Recommendation	Include the environment information as required input in the appropriate Stage Gate reviews.				
Source(s)	**CALT:** doc23938 FEPS Testing Playbook				
OE-1		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 2	**Completeness:** A responsibility matrix for the environments for testing is not identified.	**4**	**3**	**12**	**Moderate**
Finding Detail	The responsibility matrix for the management of the readiness and operation of the testing environment is not identified				
Potential Impact	If the information is not available, then confusion over the appropriate use of the environments may lead to conflict in testing and delivery of the code leading to schedule delays.				
Recommendation	Identify the responsible individual for the management of the environments.				
Source(s)	**CALT:** doc23938 FEPS Testing Playbook				
IV&V Task: OE-11	**Evaluate the historic availability and reliability of the system including the frequency and criticality of system failure.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Completeness:** Not enough information is provided about the FEPS Environments usage in the Testing Playbook.	**5**	**4**	**20**	**High**
Finding Detail	There are many facets of environments utilization that need to be commonly known to all stakeholders that are not discernible in Slide 66 and Slide 68, Environments - Regions (Development, Testing, Implementation, and Production).				
Potential Impact	If an environment usage schedule is not defined, agreed-on, published and adhered to, then unscheduled events will occur which may cause scheduling disruptions affecting the continued deployment of the system from one testing environment to another.				

Recommendation	An Environment usage schedule needs to be published, containing: • Who - the contractor(s) currently testing in each environment • What - the service(s) or testing windows for each service currently undergoing testing in each environment ○ Related code build deployment information • When – the scheduled timeframe for the anticipated testing cycle in each environment • How - List constraints, dependencies, interdependencies, conflicts if when a particular service is being tested [i.e., when a unique service is being tested (Medicaid), the environment will not be available for testing] • Scheduled outages.				
Source(s)	**CALT:** doc23938 FEPS Testing Playbook				
IV&V Task: OE-12	**Evaluate the results of any volume testing or stress testing.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Completeness:** There is no evidence of the environment to be used for stress testing in the Testing Playbook.	**3**	**4**	**12**	**Moderate**
Finding Detail	Slides 50 – 52 provide information for the planning and execution of stress testing, but do not include environment information for the stress test.				
Potential Impact	If the environment for stress testing is not identified, then there may be conflicts when a particular service is being tested leading to cost and schedule impacts.				
Recommendation	The Testing Playbook should include the test environment information on the stress test slides along with the responsible party for having the environment available and ready for stress test.				
Source(s)	**CALT:** doc23938 FEPS Testing Playbook				

2.3 SYSTEM AND ACCEPTANCE TEST

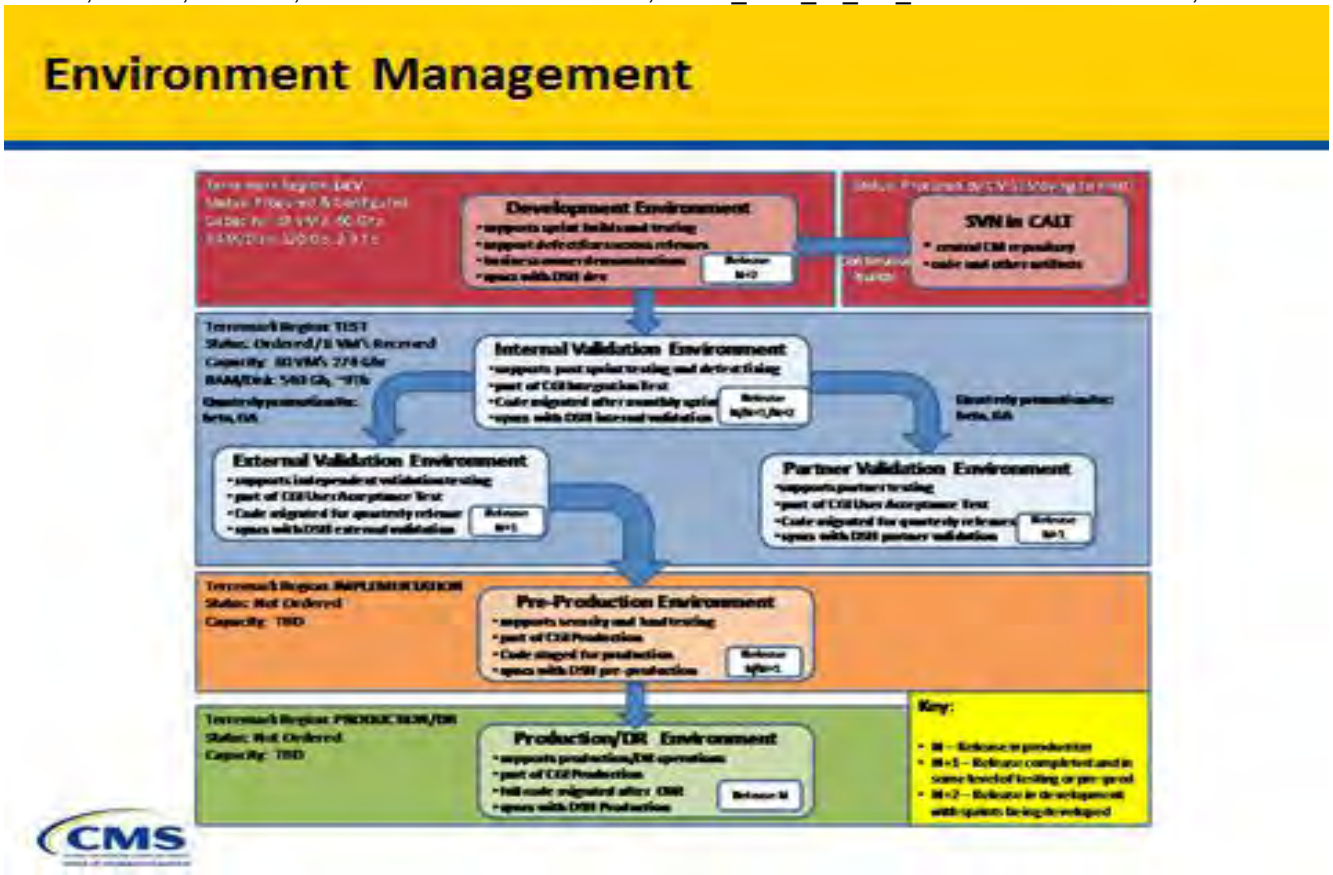
Table 2-1 System And Acceptance Test Findings

IV&V Task: ST-1	Evaluate the plans, requirements, environment, tools, and procedures used for integration testing of system modules.	Prob (P)	Impact (I)	Risk Score (P x I)	Risk Level
Finding 1	**Positive Finding**: The FEPS Testing Playbook is an excellent strategic initiative to meet the business need to identify all major gate reviews, hand-offs, coordination points and organizational roles and responsibilities for supporting both internal and external testing activities.	**N/A**			
Finding Detail	By identifying the major gate reviews, hand-offs, coordination points and organizational roles and responsibilities for supporting both internal and external testing activities, the FEPS Testing Playbook provides a much needed management tool for the testing organization.				
Potential Impact					
Recommendation					
Source(s)	**CALT:** doc23938 FEPS Testing Playbook				
ST-1		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 2	**Readability**: The IV&V team found that the ease to which the document can be read and understood is not optimal.	**4**	**3**	**12**	**Moderate**
Finding Detail	The readability of a program is related to its maintainability, and is thus a critical factor in overall software quality. The 'FEPS Testing Playbook v0 33 03 12 13.ppt' is a 97-page PowerPoint which may not be in a useful format; It does not contain a Table of Contents or a way to group related subjects for quick reference to offer the ability to address specific concerns related to FEPS Testing.				
Potential Impact	If the FEPS Testing Playbook is not organized correctly then it will not be a useful reference to its intended audience and there will be confusion in how and in what state of testing referenced activities should be embarked upon. In its present format, the Testing Playbook may not meet its intended goal of coordinating the testing efforts of internal and external parties, to ensure testing artifacts, hand-offs, and milestones are well understood and documented.				

Recommendation	Make the Testing "Playbook" into a "book"; Re-do the FEPS Testing Playbook into a Word document and re-arrange it in a more useful format to permit its purposeful use to: • Act as the primary source of CMS guidance when it comes to performing all testing processes, milestones/gate reviews, artifacts, and documents. • Act as a "living" document to identify all major gate reviews, hand-offs, coordination points and organizational roles and responsibilities for supporting both internal and external testing activities. • Design streamlined processes for the different stages and types of testing (Developer Unit, Internal, External, Performance Stress, End-to-End, and Production Readiness), etc.				
Source(s)	**CALT:** doc23938 FEPS Testing Playbook				
ST-1		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 3	**Correctness:** The DRR milestone purpose is used as the TRR milestone purpose.	**2**	**2**	**4**	**Low**
Finding Detail	Slide 15, TRR, has the same purpose as the DRR (Slide 14).				
Potential Impact	If the purpose is not stated correctly, then there can be confusion as to the purpose of the TRR.				
Recommendation	Rewrite the TRR purpose to reflect the inputs and purpose of the milestone.				
Source(s)	**CALT:** doc23938 FEPS Testing Playbook				
ST-1		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 4	**Correctness:** Separation of the TRR and TEX milestones leads to delays in testing events.	**3**	**4**	**12**	**Moderate**
Finding Detail	The TRR and TEX milestones cover the same areas and serve the same purpose. The schedule for the event leads to delays in the actual scheduled start of testing that is unnecessary.				
Potential Impact	If the TRR and TEX are not combined then there is confusion on when events actually need to take place and the result is delay in schedule and lack of use of the time during the testing period.				
Recommendation	Combine the two milestones into a single TRR and use this milestone as the start of the testing events.				
Source(s)	**CALT:** doc23938 FEPS Testing Playbook				
ST-1		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 5	**Correctness:** MIDAS is not included as a responsible stakeholder in any of the Testing Playbook milestone activities.	**4**	**2**	**8**	**Moderate**
Finding Detail	MIDAS provides inputs for testing activities and needs to be included as a participant in milestone activities.				
Potential Impact	If MIDAS is not included in related milestone activities, then data provided or used in testing may not be available for the testing event.				
Recommendation	Include MIDAS as a stakeholder in the appropriate milestone activities in the Testing Playbook.				

Source(s)	**CALT:** doc23938 FEPS Testing Playbook				
IV&V Task: ST-2	**Evaluate the level of automation and the availability of the system test environment.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Completeness:** The use of Quick Test Pro (QTP) for automation in the End to End testing phase is mentioned and the amount of automated testing is not addressed.	**3**	**3**	**9**	**Moderate**
Finding Detail	The use of Quick Test Pro for User Interface (UI) End to End testing is mentioned but not discussed as to any particulars in slides 57 and 70. It is unclear whether automated testing will actually occur.				
Potential Impact	If the use of QTP is not clearly defined and scheduled then the testing may be conducted manually increasing the time need to complete testing.				
Recommendation	If QTP is to be used for UI testing then it should be included in the schedule and tracked the same as other testing development milestones.				
Source(s)	**CALT:** doc23938 FEPS Testing Playbook				
ST-2		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 2	**Completeness:** It is unclear if Load Runner will be used as an automation tool for performance testing.	**2**	**2**	**4**	**Low**
Finding Detail	Slide 70 (Process Improvements) states the use of Load Runner for performance test is being explored. Performance testing requires a testing tool in order to execute successful testing.				
Potential Impact	If Load Runner is not available for performance testing, then performance testing may not be completed according to schedule.				
Recommendation	Decide upon the use of Load Runner or a possible replacement tool for performance testing.				
Source(s)	**CALT:** doc23938 FEPS Testing Playbook				
IV&V Task: ST-3	**Verify that an appropriate level of test coverage is achieved by the test process, that test results are verified, that the correct code configuration has been tested, and that the tests are appropriately documented, including formal logging of errors found in testing.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Completeness**: It is not clear what functionality is delivered by each contractor in each Sprint.	**4**	**3**	**12**	**Moderate**
Finding Detail	It is not clear what functionality is delivered by each contractor for each Sprint (i.e., Slide 21, Internal Testing – Process Sprint Level Test, etc.). To fulfill one of its intended purpose to "…Act as the sole source of CMS guidance when it comes to performing all testing processes, milestones/gate reviews, artifacts, and documents…", The Testing Playbook needs to list the services being deployed by a given contractor in a given Sprint to provide stakeholders with a central point of reference for FEPS service delivery.				

Potential Impact	If is not known what functionality is being delivered by each responsible contractor in a given Sprint, then it is harder to account for expected functionality in the delivered system.				
Recommendation	Expand on Slide 25 & Slide 26, Service Release FFE as of 1/23/13 by: Adding graphics depicting individual contractor schedules covering the services which are to be delivered for each Sprint (listed in the Release Management Schedule and is an output from): • Slide 10, Internal Testing - Milestone Activities Entry • Slide 11, Internal Testing - Milestone Activities Requirements Allocation (RA) • Slide 12, Internal Testing - Milestone Activities Refactoring, etc.				
Source(s)	**CALT:** doc23938 FEPS Testing Playbook				
ST-3		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 2	**Process Deviation:** The Testing Playbook's graphic depicting code deployment to 'Environments' is a deviation from the Software build/deployment methodology as referenced in the FEPS_ALM_CI_CD_Processes.ppt.	**4**	**4**	**16**	**High**

Finding Detail	For example: The Partner Validation environment flow is not captured in the Testing Playbook Slide 66, Environments, FEPS Testing Playbook Slide 8, Slide 9, Slide 10, Slide 11 - CI Software Builds, FEPS_ALM_CI_CD_Processes and Slide 13, Environment Management. 
Potential Impact	If established processes for code promotion and delivery are not consistently upheld, then there may be no reliability that the correct code configuration was deployed for a given release; hence, the delivered functionality may not satisfy or meet the expected business needs.
Recommendation	Reconcile the code promotion process differences between that presented in the Testing Playbook and in the "FEPS_ALM_CI_CD_Processes" document.

Source(s)	**CALT:** doc23938 FEPS Testing Playbook doc13095 FEPS_ALM_CI_CD_Processes				
ST-3		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 3	**Accuracy:** The internal process defect management diagram appears to be incorrect in relation to change requests (CR). (Slide 60, Defect Management – Internal Process)	**4**	**3**	**12**	**Moderate**
Finding Detail	The internal defect management process diagram (Slide 60, Defect Management – Internal Process) needs be revised to reflect the following: • When an identified defect has been determined to necessitate a requirement change (i.e., it goes back to Stakeholders and if they are in agreement), it ceases life as a defect and becomes a change request (CR) (i.e., it goes before the CCB and has been approved) Also, quality measures are not referenced to ensure an adequate defect management process is in place (i.e., assignment of proper severity levels; the introduction of resolved deferred defects into the code resolution lifecycle, etc.).				
Potential Impact	If a defect is not accurately portrayed as a CR, then an unapproved change to a requirement may be implemented.				
Recommendation	Review the defect process documentation and ensure that defects that make a requirement change are handled as CRs and update Slide 60				
Source(s)	**CALT:** doc23938 FEPS Testing Playbook doc13095 FEPS_ALM_CI_CD_Processes				
ST-3		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 4	**Consistency:** The use of the term ‘defect’ does not appear to conform to IEEE standards in order to avoid confusion to the term ‘change request’.	**3**	**3**	**9**	**Moderate**

Finding Detail	In the Testing Playbook, defects are construed as being synonymous to change requests.
	• Slide 60, Defect Management – Internal Process
	• Slide 62, Defect Management – External Process
	• Slide 65, Defect Management – External Communications Plan, Vendor Defect / Change Management Tool
	
	Defects and Change Requests (CRs) have their own lifecycle, (each) which introduces code enhancements or corrections into the code deployment processes.
	• CRs are usually requirements change work items (tasks) or enhancements
	  ○ Related tasks - review and adjudicate (approve or reject/escalate) CR's to base-lined items that significantly impact IT scope, schedule, or cost and affect one or more business areas; they may occur:
	  ▪ Within the SDLC
	  ▪ In Production
	
	Defects - the application does not work as desired or as expected (as in a bug needing to be fixed)
	• Defects originate from inside and outside the SDLC
	  ○ Requirements
	  ○ Code
	  ○ Test
	  ○ Production – "hot fixes", regular, etc.				

Potential Impact	If the difference between defects and change requests is not clear, then changes may be made to requirements without CCB approval.				
Recommendation	Use standardized terminology for defect and change management which will allow freedom from contradiction among the documents or parts of a system or component (IEEE 1012). Review the software products to detect defects in the specified work products at each selected development activity to assure the quality of the emerging software.				
Source(s)	**CALT:** doc23938 FEPS Testing Playbook **Standard:** IEEE-829 Sys Test IEEE Std. 829-2008 IEEE Standard for Software and System Test Documentation				
ST-3		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 5	**Completeness:** The external process defect management diagram appears to be incorrect (Slide 62, Defect Management – External Process) with regard to change requests (CR).	**4**	**4**	**16**	**High**

Finding Detail	The external defect management process diagram (Slide 62, Defect Management – External Process) needs revision to reflect the following: • At the bottom right of the graphic, in the 'Vendor Actions' area - when the 'Tier 2 defect ticket' has been assigned to a particular vendor and the vendor has reviewed and updated the ticket, it should not be shown that the vendor creates a CR; the decision is up to the CCB (it goes before the CCB, and if approved, the defect becomes a CR); it is not up to the vendor to assignment the defect as a CR. Once approved, the CR would go to the development team code build process flow as an emergency fix or in a scheduled build for eventual deployment. Also, Slide 65, Defect Management – External Communications Plan, Vendor Defect / Change Management Tool also has to be updated to reflect CCB's involvement in the CR creation process.				
Potential Impact	If the review process for the Vendor is maintained as the slide shows, then the Vendor may be in control of creating change requests and result in increased project costs.				
Recommendation	Review the defect process documentation and ensure that the vendor participation in the defect process is accurately portrayed and update Slide 62.				
Source(s)	**CALT:** doc23938 FEPS Testing Playbook doc13095 FEPS_ALM_CI_CD_Processes				
ST-3		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 6	**Completeness:** Contact information is missing from the organization chart provided in Slide 4 (Testing Points of Contact).	2	2	4	**Low**
Finding Detail	Slide 4 is for Testing Point of Contact information and does not provide the information needed for contacting the members identified in the organization chart.				
Potential Impact	If point of contact information is not available, then the Testing Playbook does not serve as the sole source for testing information.				
Recommendation	Add the appropriate contact information to Slide 4				
Source(s)	**CALT:** doc23938 FEPS Testing Playbook				
ST-3		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 7	**Completeness:** Decision points and communication processes are not reflected to support the testing POCs in Slide 4 of the Testing Playbook.	3	4	12	**Moderate**
Finding Detail	Testing decision points and communication processes need to be identified for testing activities during the life cycle process as depicted in the Testing Playbook.				
Potential Impact	If communications channels between internal & external teams and external suppliers are not clearly defined and advocated to deal with the defects, risks, and issues detected during the transition process, then it will be confusion on who to contact when problems occur and it will be difficult to create timely resolution paths during the systems' transition.				

Recommendation	Define and maintain suitable communication channels between internal teams and external suppliers to deal with the defects, risks, and issues detected during the transition process (as ITIL advocates pg. 241).				
Source(s)	**CALT:** doc23938 FEPS Testing Playbook **Standards:** ITIL V3 Intermediate - Service Transition				
IV&V Task: ST-9	**Verify that the test organization has an appropriate level of independence from the development organization.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Positive Finding:** The test organization chart shows the test team reports to the executive team.	N/A			
Finding Detail	Slide 4 is the test organization chart and displays the FEPS testing organization report levels go directly to the executive team				
Potential Impact	None				
Recommendation	None				
Source(s)	**CALT:** doc23938 FEPS Testing Playbook				
IV&V Task: ST-11	**Acceptance procedures and acceptance criteria for each product must be defined, reviewed, and approved prior to test and the results of the test must be documented. Acceptance procedures must also address the process by which any software product that does not pass acceptance testing will be corrected.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Completeness:** Entry and exit criteria for Stage Gate and Checkpoint Reviews are not addressed.	**4**	**4**	**16**	**High**
Finding Detail	Each identified Testing Playbook activity (milestone and others) has an input and an output; the outputs need to be presented as deliverables or work products to be evaluated. Feedback needs to be provided for timely remediation (on deviations and unexpected results) prior to commencing to the next logical lifecycle event. Slide 16 Internal Testing - Milestone Activities for Internal Validation Readiness Review (IVRR), Slide 17 Internal Testing - Testing Execution (TEX), Slide 18 Internal Testing - Test Analysis (TA), Slide 19 Internal Testing - Close Out (TCO), Slide 20 Internal Testing - External Validation Readiness Review (EVRR) Slide 31 External Testing – Milestone Activities for QHP Readiness Determination (RD Slide 38 External Testing – Milestone Activities for State Partner Test Readiness Review (TRR) Slide 41 External Testing – Milestone Activities for State Partner SBE Readiness Determination (RD) The Slides do not identify what constitutes acceptance for moving forward into the next test phase.				

Potential Impact	If the entry and exit criteria on software products are not explicitly defined, documented, reviewed, approved and fully understood prior to test, and if the criteria is not upheld, then the result may be slipped schedules ,increased costs, and result in a lower quality product.				
Recommendation	Document, agree on and enforce acceptance procedures for Stage Gate reviews.				
Source(s)	**CALT:** doc23938 FEPS Testing Playbook				
ST-11		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 2	**Completeness:** Number of acceptable defects and severity levels not addressed in Stage Gate Review slides	**3**	**4**	**12**	**Moderate**
Finding Detail	The acceptable number of defects and severity level for open defects should be part of the Stage Gate review exit criteria.				
Potential Impact	If the status of defects and the acceptable level of defects are not included in the Stage gate review exit criteria, then the delivered system may contain show stopper defects that prevent the successful completion of the next stage.				
Recommendation	In the Stage Gate review slides include the criteria for review and the acceptability of defects in the program as part of the Outputs section.				
Source(s)	**CALT:** doc23938 FEPS Testing Playbook				
ST-11		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 3	**Completeness:** There is no indication of a process in place for the failure of a Stage Gate review.	**3**	**5**	**15**	**High**
Finding Detail	There is no indication of a process in place for the failure of a Stage Gate review. Processes and procedures need to be identified for a Stage Gate review that fails to meet the acceptance criteria for the Stage Gate.				
Potential Impact	If there is no process in place to handle the failure to meet the Stage Gate, then the process may be performed incorrectly and incompletely.				
Recommendation	Develop a slide to provide the steps required when there is a failure of a Stage Gate Review.				
Source(s)	**CALT:** doc23938 FEPS Testing Playbook				
ST-11		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 4	**Completeness:** Process should be identified for how performance testing results will be incorporated into the subsequent rounds of stress test.	**3**	**4**	**12**	**Moderate**
Finding Detail	Slide 54 (External Testing Flow, Performance Stress Test) provides the external Testing Flow for the performance stress test but does not include how performance testing results will be incorporated into the subsequent rounds of stress test to improve baseline timings for services between partners, under specific transaction loads, and to identify and resolve bottlenecks that may affect performance and capacity planning to optimize overall system performance				

Potential Impact	If performance testing results information is not included in the flow, then procedures for handling subsequent rounds of stress test to improve baseline timings for services between partners, under specific transaction loads, and to identify and resolve bottlenecks that may affect performance and capacity planning to optimize overall system performance may not be developed and performance Stress testing issues may impact the overall schedule.				
Recommendation	Update Slide 54 to include the information for how performance testing results will be incorporated into the subsequent rounds of stress test to improve baseline timings for services between partners, under specific transaction loads, and to identify and resolve bottlenecks that may affect performance and capacity planning to optimize overall system performance				
Source(s)	**CALT:** doc23938 FEPS Testing Playbook				
ST-11		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 5	**Process Improvement:** Testing Playbook should reference testing activities as part of the IMS.	**3**	**3**	**9**	**Moderate**
Finding Detail	Unrealistic and aggressive schedule mandated by ACA legislation causes strict time constraints on the project delivery without the benefit of the timeframe needed to fully remediate issues and regression test corrective code. Given FEPS' imminent implementation containing emergent wide-ranging systems, stood-up by new technologies, unconfirmed functional environments along with delayed delivery schedules, configuration issues with tools and hardware, resulting in an overall challenging assimilation of the individual systems. • Slide 66, Environments • Slide 67, Testing Environments Summary • Slide 68, Environments (Development, Sprint, Release, External Testing Timeline)				
Potential Impact	If the testing activities and milestone are not reflected in the IMS given the aggressive schedule, then any schedule impacts from testing will not be apparent to program management.				
Recommendation	Ensure the major testing events and milestones from the Testing Playbook are in the IMS so that testing visibility is increased and considered by other dependent events.				
Source(s)	**CALT:** doc23938 FEPS Testing Playbook				

2.4 OPERATIONS OVERSIGHT

Table 2-1 Operations Oversight Findings

IV&V Task: OO-5	Evaluate operational plans and processes.	Prob	Impact	Risk Score (P x I)	Risk Level
Finding 1	**Correctness:** Input and output identification and sequencing schemes are being introduced when sequence is not required.	3	2	6	Low
Finding Detail	New terms and sophisticated identification schemes for inputs, outputs and artifacts were introduced in the meeting. These items only add to the confusion and communication issues on the FEPS Program.				
Potential Impact	If stakeholders modify vocabulary and add identification schemes late in the lifecycle, then confusion may increase on the project.				
Recommendation	• Keep the vocabulary simple. • Keep FEPS Program acronyms and definitions in CALT and update them as needed.				
Source(s)	**CALT:** doc23938 FEPS Testing Playbook **Meeting:** DRR on 3/25/2013				
OO-5		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 2	**Completeness:** Information is not provided about backup and restore activities to support the Internal & External test infrastructure.	5	4	20	High
Finding Detail	It is not clear whether backup and restore service activities are listed as necessary activities in the Playbook, so as to make available, artifacts, test harnesses, etc., in the event of significant disruptions in the FEPS Testing infrastructure.				
Potential Impact	If backup and restore procedures are not identified in the Testing Playbook, then a failure of the environment may lead to the loss of data and have a major impact on the testing schedule leading to delay in the delivery of production ready code.				
Recommendation	Include backup and restore procedures and guidelines in the Testing Playbook.				
Source(s)	**CALT:** doc23938 FEPS Testing Playbook doc12881 Backup and Restore Services_				

APPENDICES

APPENDIX A: ACRONYMS

Acronyms used in this document are listed below.

Acronym	Description
ACA	Patient Protection and Affordable Care Act
CALT	Collaborative Application Lifecycle Tool
CIISG	Consumer Information & Insurance Systems Group
CMMI	Capability Maturity Model Integration
CMS	Centers for Medicare & Medicaid Services
DDR	Detailed Design Review
FEPS	Federal Exchange Program System
FFE	Federally Facilitated Exchange
IEEE	Institute of Electrical and Electronics Engineers
IMS	Integrated Master Schedule
IT	Information Technology
ITIL	Information Technology Infrastructure Library
IV&V	Independent Verification and Validation
N/A	Not Applicable
OE	Operating Environment
OO	Operations Oversight
PMBOK	Project Management Institute's Project Management Body of Knowledge
QHP	Quality Health Plan
RMP	Risk Management Plan
SOW	Statement of Work
ST	System Testing
V&V	Verification and Validation
W3C	World Wide Web Consortium (W3C)
XLC	Expedited Life Cycle

APPENDIX B: STAKEHOLDERS INTERVIEWED

Table B-1 Interviews & Meetings

There were no interviews or meetings for this assessment. It is limited to documentation only.

APPENDIX C: DOCUMENTATION REVIEWED

Table C-1 Documentation Reviewed

Document Element #	Document ID #	Document/Information Received	Source
D01	doc23938	FEPS Testing Playbook	CALT
D02	doc13095	FEPS_ALM_CI_CD_Processes	CALT
D03	doc4380	FFE Quality Management Plan_v1.0_Final Draft	CALT
D04	doc4371	CMS Federal Facilitated Exchange Project Management Plan_v1.0_02062012a	CALT
D05	N/A	Document Readiness Review (DRR) on 3/25/2013	Meeting
D06	N/A	Test Execution Review (TEX) on 4/16/2013	Meeting

APPENDIX D: RISK DETERMINATION

D.1 RISK DESCRIPTION

Findings identified in this assessment must be associated with several metrics factors to help determine the level of risk value related to a specific element or process. Risk is defined as the combination of the probability of occurrence and the consequences of a given future undesirable event. Risk can be associated with products and/or projects.

The determination of risk or vulnerability can be expressed as a function of:

- The likelihood (probability) of a given finding posing a risk to system development or functionality
- The magnitude of the impact of a finding posing a risk to system development or functionality

Where:

P = Probability
I = Impact
and: P x I = Risk Score

To measure risk, a risk scale and a risk-level matrix has been developed.

D.2 RISK DETERMINATION

Table D-1 displays the Risk Scale and required actions. This risk scale, with its ratings of High, Moderate, and Low, represents the degree or level of risk to which a system, facility, or procedure might be exposed to a given vulnerability were exercised. The risk scale also presents actions that senior management, the mission owners, must take for each risk level.

Table D-1 Risk Scale and Necessary Actions

Risk Rating	Action Implementation
High	High-risk levels create a strong need for corrective actions and the creation of an action plan that is put in place as quickly as possible.

Risk Rating	Action Implementation
Moderate	Moderate-risk levels warrant corrective actions and a plan to incorporate those actions within a reasonable period of time.
Low	For low-risk levels, the application owner must decide whether corrective actions are needed or whether the risks may be accepted.

D.3 RISK MITIGATION AND RECOMMENDATIONS

During the risk mitigation process, controls that could mitigate or eliminate the identified risks are provided. The goal of the recommended controls is to reduce the level of risk to FEPS and its data to an acceptable level. The following factors should be considered in recommending controls and alternative solutions to minimize or eliminate identified risks:

- Effectiveness of recommended options (e.g., system compatibility)
- Organizational policy
- Operational impact

For consistency and clarity and to maintain an accurate understanding of risk findings, IV&V adopted the CMS risk management methodology, as defined in the Risk Management Plan (CMS RMP – '*CMS Health Insurance Exchange Risk Management Plan v 1.1_04302012_Draft'*); accordingly, risks identified on the FFE project level will be shared with partner and stakeholder groups for visibility and shared understanding of FEPS project risks to support successful risk management at the project level and through the enterprise level through correlation to the FFE Integrated Master Schedule (IMS) milestones and tasks. The intent is to identify and appropriately address and elevate project risks to the Health Insurance Exchange Program level for visibility, mitigation and for possible action.

Each risk is documented as fully as possible to include probability (likelihood), impact, risk value, system & scope assessment area and overall characteristic. As a part of the documentation of the risk, a nominal probability (likelihood) and impact rating on the risk finding was submitted and was mathematically factored to reach an overall risk value. See Tables 2-3, 2-4, and 2-5 for probability, impact and risk value guidance.

Table D-2 Probability Assessment Criteria

Level	Probability	Probability of Occurrence
5	Near Certainty	81-99%
4	Highly Likely	61-80%
3	Likely	41-60%

Level	Probability	Probability of Occurrence
2	Low	21-40%
1	Not Likely	5-20%

Table D-3 Impact Assessment Criteria

Level	Impact
5	Severe degradation in technical threshold performance; jeopardizes project success. Cannot meet key milestones. Represented as a 20% deviation of the baselined plan.
4	Significant degradation in tech performance, unacceptably below goals, no design margins. Requires program or project critical path change. Represented as a 15–20% deviation of the baselined plan.
3	Moderate shortfall in tech performance, with limited impact; technical goals unmet and design margins significantly reduced. Schedule slip impacts milestone (MS) or Critical path slack. Represented as a 10–15% deviation of the baselined plan.
2	Minor reduction in technical performance, but can be tolerated, little impact; goals and design margins reduced. Schedule slip but will meet MS. Represented as a 5–10% deviation of the baselined plan.
1	Minimal consequence to performance, but no overall impact; goals and design margins will be met. No schedule slip. < 1% increase from baseline.

Table D-4 Risk Value

Risk Value Exposure Score	Risk Level
15-25	High
6-14	Moderate
1-5	Low

Exhibit 13

TurningPoint. Federal Marketplace Program System (FMPS) Independent Verification & Validation (IV&V) Assessment 8 Report. June 10, 2013.

CENTERS FOR MEDICARE & MEDICAID SERVICES

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

Federal Marketplace Program System (FMPS)

Independent Verification & Validation (IV&V) Assessment 8 Report (Cloud Computing)

Version 1.0

June 10, 2013

Prepared by:

TurningPoint
TurningPoint Global Solutions
Software Services Company™

Document Number: FEPSIVV-IAR-08
Contract Number: HHSM-500-2012-00008U

APPROVALS

Exchange IT Program Approving Authority:

Signature Printed Name Date Phone Number

Monique Outerbridge, CMS/OIS/CIISG, Director

Signature Printed Name Date Phone Number

Mark Oh, CMS/OIS/CIISG, Division of Enterprise Architecture and Requirements Management Director

Signature Printed Name Date Phone Number

[redacted] CMS/OIS/CIISG, Government Task Lead

REVISION HISTORY

Version	Date	Organization/Point of Contact	Description of Change
1.0	06/10/2013	TurningPoint	Initial submission

Table of Contents

EXECUTIVE SUMMARY 1

1 INTRODUCTION 4

1.1 BACKGROUND 4
1.2 SCOPE 4
1.3 FMPS OVERVIEW 4
1.4 IV&V APPROACH AND METHODS 4
1.5 ASSUMPTIONS 5
1.6 CONSTRAINTS 5
1.7 REFERENCES 5

2 CLOUD COMPUTING FINDINGS 6

2.1 CLOUD COMPUTING FINDINGS - REQUIREMENTS MANAGEMENT 6
2.2 CLOUD COMPUTING FINDINGS - OPERATING ENVIRONMENTS 19
2.3 CLOUD COMPUTING FINDINGS - SYSTEM AND ACCEPTANCE TEST 37
2.4 CLOUD COMPUTING FINDINGS - OPERATION OVERSIGHT 39

APPENDICES 53

APPENDIX A: ACRONYMS 54

APPENDIX B: STAKEHOLDER INTERVIEW/MEETING 56

APPENDIX C: REVIEWED DOCUMENTATION 57

APPENDIX D: RISK DETERMINATION 59

D.1 RISK DESCRIPTION 59
D.2 RISK DETERMINATION 59
D.3 RISK MITIGATION AND RECOMMENDATIONS 60

Figures

Figure 1: Findings by Scope of Service Area 2
Figure 2: Total Findings by Risk Level 3

Tables

Table 1: Findings by IV&V Service Area 2
Table 2-1 Cloud Computing Findings - Requirements Management 6
Table 2-2 Cloud Computing Findings - Operating Environments 19
Table 2-3 Cloud Computing Findings - System and Acceptance Test 37
Table 2-4 Cloud Computing Findings - Operation Oversight 39

Table B-1 Interviews and Meetings 56
Table C-1 Reviewed Documentation 57
Table D-1 Risk Scale and Necessary Actions 59
Table D-2 Probability Assessment Criteria 60
Table D-3 Impact Assessment Criteria 61
Table D-4 Risk Value 61

EXECUTIVE SUMMARY

This report presents the results of the seventh assessment by the Independent Verification & Validation (IV&V) contractor, TurningPoint Global Solutions, which was tasked by the Centers for Medicare and Medicaid Services (CMS) to provide technical audits of the Federal Marketplace Program System (FMPS). The team focused on cloud computing for this assessment. The National Institute of Standards and Technology (NIST)'s definition of cloud computing (available at: http://csrc.nist.gov/groups/SNS/cloud-computing) is: a model for enabling available, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services). The major benefit is that these resources can be rapidly provisioned and released with minimal management effort or service provider interaction.

CLOUD TECHNICAL REQUIREMENT CONCERNS

The IV&V Team interviewed Terremark, and reviewed the available relevant documentation, and had the following concerns with respect to Infrastructure as a Service (IaaS) cloud capabilities that are *not* provided by Terremark for FMPS:

- On-demand self-service - A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service's provider.
- Ubiquitous network access - Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs).
- Rapid elasticity - Capabilities can be rapidly and elastically provisioned to quickly scale up and rapidly released to quickly scale down. To the consumer, the capabilities available for provisioning often appear to be infinite and can be purchased in any quantity at any time.
- Measured Service - Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported providing transparency for both the provider and consumer of the utilized service.

Platform as a Service (PaaS) is defined by NIST as the capability provided to the consumer to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment. The IV&V Team found that PaaS services are being provided through the leveraging of Collabnet TeamForge which supports Agile Application Lifecycle Management; however, the services are provided in the CMS Private Cloud with the constraints noted above.

The IaaS technical requirements are normally available in the cloud environment, but are unavailable or restricted in the FMPS private cloud environment, and could result in inefficient use of government resources in operating and maintaining the Program.

FINDINGS OVERVIEW

The IV&V findings are spread somewhat evenly across the IV&V Requirements, Operating Environment and Operations Oversight service areas. The majority of the high findings are in the Operating Environment and Operations Oversight service areas. Of specific concern are the following:

- The lack of elasticity in resource utilization.
- Inadequacy of the Disaster Recovery site.
- Inadequate backup status reporting.
- Inadequacy of the current hardware configurations.
- The lack of Federal Information Security Management Act (FISMA) compliance.
- Missing elements in the capacity planning document and capacity planning.
- The lack of an Information Technology Infrastructure Library (ITIL) -compliant problem management process, and the inconsistent performance of root-cause analysis.

Table 1 shows the total findings with risk values, by IV&V service areas for this assessment only.

Table 1: Findings by IV&V Service Area

Total Findings				
	Low	Moderate	High	Total
IV&V Service Area				
Requirements Management	4	7	3	14
Operating Environment	3	12	4	19
System and Acceptance Testing	0	0	0	0
Operations Oversight	3	10	5	18
Total	10	29	12	**51**

Figure 1 displays a summary of findings for this assessment, with a distribution of risk levels. A description of the determination of risk levels appears in Appendix D: Risk Determination.

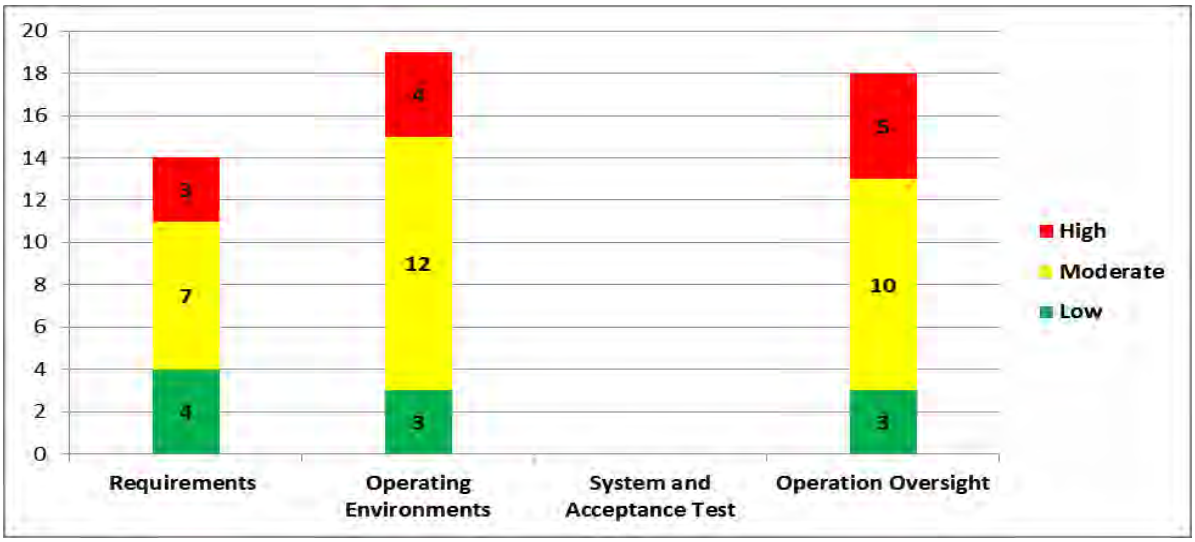


Figure 1: Findings by Scope of Service Area

Figure 2 displays a summary of total findings by risk level.

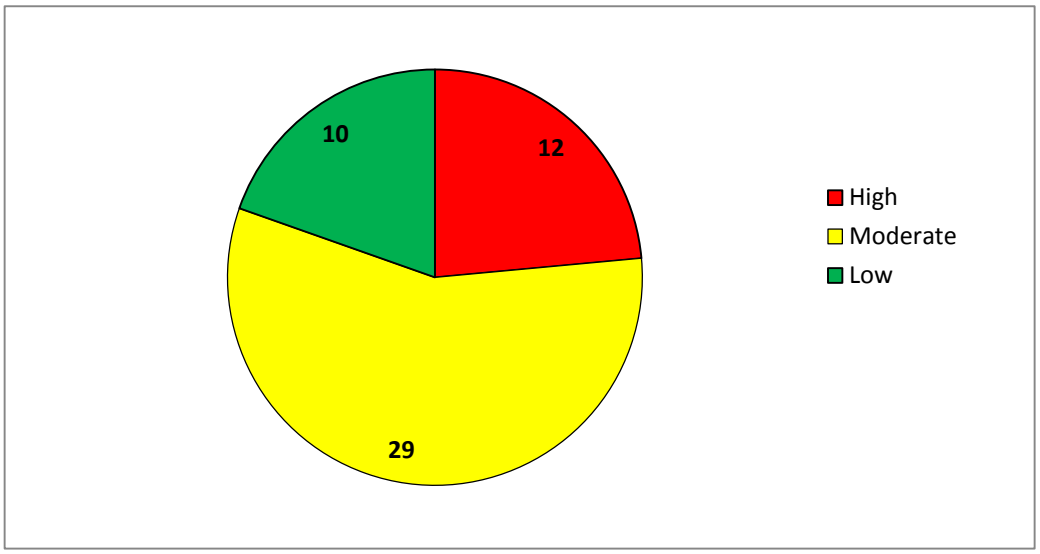


Figure 2: Total Findings by Risk Level

RECOMMENDATIONS

The IV&V Team recommends the following:

1. ***Capacity*** - Terremark General Support System (GSS) and the Infrastructure are in an operational system status (pg.8 Center-for-Consumer-Information-and-Insurance-Oversight-TMRK_CSP4IaaS-999-SSP-08-30-2012); thus, it is particularly important that a capacity plan is in place to avert production problems. CMS and relevant contractors should carry out a capacity planning lifecycle exercise (and provide the artifacts in CALT) to address the current business requirements and to also forecast future processing requirements.
2. ***Capacity*** - Document the model used for forecasting demand, the methods to differentiate the trend from spikes in demand, and how Infinicenter is used to report on any spikes or rises in demand.
3. ***Security*** - Ensure Plan of Action and Milestones (POAMs) are met by the due date and take steps immediately to mitigate residual security risk. Before hosting sensitive application data, ensure that these POAMs are closed.
4. ***Disaster Recovery*** - Provide a failover site with the same configuration as the primary site to meet 24x7 operations. Ensure processes and procedures exist to synchronize primary site data files with failover site data files, to ensure that when primary site is lost, the failover site can take over right away.
5. ***Backup*** - Review the backup and recovery procedures, make decisions on which method should be used and update the documents to ensure files are consistent in backup/restore methodology.
6. ***Incident Management*** - Update section 4 of the Incident Management Plan including the trend analysis process, communication process among the teams that must pool their knowledge and expertise to diagnose and resolve the problem, and the process for setting up priority levels to ensure there is efficient allocation of resources.

1 INTRODUCTION

1.1 BACKGROUND

The FMPS program was initiated by CMS to provide health insurance exchange capabilities required by the Patient Protection and Affordable Care Act (ACA) of 2010. In support of the FMPS effort, CMS employed TurningPoint to provide an independent and unbiased analysis of the FMPS components and artifacts. CMS tailored the IEEE 1012 standard to 106 V&V service areas covering the nine Scope of Service areas in the FMPS IV&V SOW: Quality Management, Training, Requirements Management, Operating Environment, System and Acceptance Testing, Data Management, and Operations Oversight. Not all service areas will be covered in all assessments.

1.2 SCOPE

The scope of this assessment is focused on documents and artifacts related to the cloud computing environment as well as interviews with CMS and Terremark personnel.

1.3 FMPS OVERVIEW

The IV&V team analyzed and organized the assessment of FMPS cloud computing in the following areas:

- System Requirements identified for normal and abnormal operation within the Terremark Cloud.
- Operating Environment
- System testing of platforms to assess readiness and availability
- Operations Oversight

1.4 IV&V APPROACH AND METHODS

Our approach is structured and includes: planning the scope of the assessment, requesting pertinent documentation, conducting interviews, participating in program meetings, and identifying early warning signs and areas of risk to focus the assessment depth. The IV&V approach to working with federal and contractor organizations is cordial and supportive of priorities, while maintaining independence and objectivity during the assessment.

The IV&V team used CALT to identify the artifacts related to the scope of the assessment, and then used the IV&V service areas and the IV&V checklist to develop questionnaires for missing information. After reviewing the documentation, follow-up interviews were conducted to gather more detailed information.

The findings are categorized by system and presented in tables. Each finding includes an IEEE categorization, impact statement, sources, risk probability, risk impact, and risk value. Please see Appendix D: Risk

Determination for more detailed information about the method used to determine risk impact, probability and value.

1.5 ASSUMPTIONS

The IV&V team made the following assumptions during this assessment:

- CALT is the repository of operational and security documentation for operations related to cloud computing in the Terremark environments.
- CMS and contractor staff have provided accurate and current information during interviews, meetings and questionnaires.

1.6 CONSTRAINTS

The IV&V team was constrained by the following during this assessment:

- There was no access to Infinicenter for analysis of reports related to cloud computing operations.
- There was no access to Remedy for analysis of incidents related to cloud computing operations.
- There was no access to the Nagios and Groundwork continuous monitoring platforms related to the cloud computing operations.
- There was one security document that could not be reviewed because it was password protected.
- The IV&V Team is not involved in critical cloud-related stakeholder meetings.

1.7 REFERENCES

The standards listed below were utilized for the IV&V team's review of the FMPS Program and in the preparation of the Assessment Report 8 (Cloud Computing).

- IEEE Standard for Software Verification and Validation 1012-2004
- IEEE Recommended Practice for Software Requirements Specifications 830-1998
- IEEE Standard 829/1998 for Software Test Documentation
- The Software Engineering Institute (SEI) Capability Maturity Model Integration (CMMI)
- Project Management Institute's Project Management Body of Knowledge (PMBOK)
- CMS Expedited Lifecycle Process (XLC)
- Section 508 Accessibility of Electronic and Information Technology
- Guidance for Exchange and Medicaid IT Systems, V 1.0 and 2.0
- Medicaid and Exchange IT Architecture Guidance

2 CLOUD COMPUTING FINDINGS

2.1 CLOUD COMPUTING FINDINGS - REQUIREMENTS MANAGEMENT

Table 2-1 Cloud Computing Findings - Requirements Management

Task: RM-6	**Evaluate and make recommendations on project policies and procedures for ensuring that the system is secure and that the privacy of client data is maintained.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Correctness:** Resource utilization is not automated as expected for IaaS private cloud services; this impacts system availability.	5	4	20	**High**
Finding Detail	In an IaaS, it is expected that there would be on-demand access of computing, networking and storage resources. This is important to the availability of FMPS, which has been designated as a "moderate" system per FIPS 199. Instead, the IV&V team found that the Terremark contract is FFP for a specific amount of resources. All elasticity changes are performed manually through contract change requests that come from CMS through the Terremark prime contractors (e.g. CGI, QSSI, and IDL) to Terremark. Although this supply chain may exist by design, it does not fit the definition of cloud services. Every approved request is implemented by using the Infinicenter GUI by URS. a. Additional RAM b. Additional Processor c. Additional Storage				
Potential Impact	If resource utilization requires lead time to purchase bandwidth, then availability requirements may not be met.				
Recommendation	Ensure capacity covers peak performance requirements at all times. Consider actually procuring cloud services.				
Source(s)	**Interview:** Cloud Computing Assessment Discussion with Terremark 05212013 Cloud Computing Assessment Discussion with Terremark 05232013				
Task: RM-6		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 2	**Completeness:** The URS Personnel Policies are still in draft form and incomplete.	3	4	12	**Moderate**
Finding Detail	The Personnel Security Policy should also define: objectives of information security, statement of management intent, risk management framework and the security incident reporting process. In addition, it should be reviewed at defined intervals and updated when significant changes occur. Also, the SOW states the following performance requirement for all deliverables, "All submissions will be 100% complete and compliant with all applicable regulations."				
Potential Impact	If the personnel security policy is not finalized and complete, then some aspects of management intent may not be communicated.				

Recommendation	• Finalize the policy document. • Perform an annual review and revise as needed. This should be documented in the revision history.				
Source(s)	**CALT:** doc12863 PaaS_SOP_Personnel Security Mgmt_09062012 **GTL:** OptYr2 Mod7 HHS SOW v11				
Task: RM-7	**Evaluate the projects restrictions on system and data access.**	**Prob. (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Positive Finding:** The IV&V Team has found evidence of project restrictions on system and data access.	**N/A**			
Finding Detail	In doc12859 chapter 3.0 SECURITY CONTROLS DETAIL AND COMMENT, there are detailed descriptions of how system and data will be accessed and what are the conditions: Access Control (AC) Controls Security Awareness and Training (AT) Controls Audit and Accountability (AU) Controls Security Assessment and Authorization Controls Configuration Management (CM) Controls Contingency Planning (CP) Controls Identification and Authentication (IA) Controls Incident Response (IR) Controls Maintenance (MA) Controls Media Protection (MP) Controls Physical and Environmental Protection (PE) Controls Planning (PL) Controls Personnel Security (PS) Controls Risk Assessment (RA) Controls System and Services Acquisition (SA) Controls System and Communications Protection (SC) Controls System and Information Integrity (SI) Controls Program Management (PM) Controls For example: (1) Infinicenter needs userid/password to log in: 5.1 User Sign-In Open an Internet web browser (either Internet Explorer 6 (preferred) or higher or Mozilla Firefox 2.0.0.9 or higher) and enter the following URL in the web browser address bar to navigate to the Infinicenter Sign In screen. http://icenter.digitalops.net *(If you have a private instance of eCloud see your service manager for the proper URL)*				

(2) Doc12381 FFE_HTD documents described the details how FFE system will be secured and controlled.

Potential Impact	N/A
Recommendation	N/A
Source(s)	**CALT**: doc12859 CFACTS CSP4 PaaS System Security Plan Final090412 doc12381 FFE_HTD doc17091 MIDAS SSP doc17090 MIDAS ISRA **GTL**: 20130426 Welcome Guide to Enterprise Cloud Federal Version LAN

Task: RM-7		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 2	**Correctness:** Doc12859 CFACTS CSP4 PaaS System Security Plan Final090412.docx is out of date. No changes were recorded in the revision log.	**4**	**1**	**4**	**Low**

Finding Detail

artf125595 states "The SSP does not contain accurate information about the controls for CALT, and some controls are not addressed at all. Major changes have occurred since the plan was published, and those changes do not appear in the current version. Without complete and updated information about the controls, it is not possible to test and verify whether the security controls are adequate to protect CALT at the necessary level. This poses a problem for the business owner who, using incomplete information, must make the decision to accept the residual risk when approving a system to operate"

See below of doc12859 page 4

REVIEW LOG

This SSP Review Log is maintained to record the reviews that have taken place for this system.

The review log should be completed by entering the data from each column in the appropriate row. The log may also be completed by using a pen.

Date of Review.	Staff Name of Reviewer	Organization of Reviewer

Potential Impact	If the SSP does not contain accurate information then it is not possible to test and verify the security controls are adequate to protect CALT at the necessary level.				
Recommendation	Update doc12859 with the latest information in CALT				
Source(s)	**CALT**: artf125595 CALT Security #19: SSP is Out of Date doc12859 CFACTS CSP4 PaaS System Security Plan Final090412				
Task: RM-7		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 3	**Correctness:** Cannot open doc12859 seven attachments in Appendixes one to seven respectively.	**1**	**5**	**5**	**Low**
Finding Detail	There are seven appendices in this document, and it all says "See attached file(s)." But no attached files can be found in these appendices. The list of all the appendices are: Appendix A - EQUIPMENT LIST Appendix B - SOFTWARE LIST Appendix C - DETAILED CONFIGURATION SETTINGS Appendix D – GLOSSARY Appendix E - ACRONYMS & ABBREVIATIONS Appendix F - ATTACHMENT 1 Appendix G - ATTACHMENT 2				
Potential Impact	If no details are provided for these seven appendices, the evaluation of the projects restrictions on system and data access cannot be made accurately. The integrity of the project could be hindered.				
Recommendation	Update all appendices in doc12859 with the latest information in CALT.				
Source(s)	**CALT**: doc12859 CFACTS CSP4 PaaS System Security Plan Final090412				
Task: RM-8	**Evaluate the projects security and risk analysis.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Positive:** There is a signed Authority to Operate (ATO) for the PaaS through 3/31/2014**.**	N/A			
Finding Detail	The platform has gone through the standard NIST C&A process (along with meeting additional CMS controls), and the residual risk was accepted by the CMS Chief Information Officer. Terremark has taken action on each of the remaining requirements: Application for FEDRAMP submitted in Nov. 2012 and a Memorandum of Understanding (MOU) between Terremark and the CMS Baltimore Data Center is				

	waiting for the signature of Monique Outerbridge as of 5/23/13. (Contingency Plan action is covered in another section of this report).				
Potential Impact	N/A				
Recommendation	N/A				
Source(s)	**GTL:** Center-for-Consumer-Information-and-Insurance-Oversight-TMRK_CSP4IaaS-ATO Memo 2013 **Interview:** Cloud Computing Assessment Discussion with Terremark 05232013				
Task: RM-8	**Evaluate the projects security and risk analysis.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 2	**Positive:** There is a signed Authority to Operate (ATO) for the IaaS through 3/31/2014**.**	N/A			
Finding Detail	The infrastructure has gone through the standard NIST C&A process, and the residual risk was accepted by the CMS Chief Information Officer. Terremark has taken action on each of the remaining requirements: Application for FEDRAMP submitted in Nov. 2012 and a Memorandum of Understanding (MOU) between Terremark and the CMS Baltimore Data Center is waiting for the signature of Monique Outerbridge as of 5/23/13. (Contingency Plan action is covered in another section of this report).				
Potential Impact	N/A				
Recommendation	N/A				
Source(s)	**GTL:** Center-for-Consumer-Information-and-Insurance-Oversight-TMRK_CSP4IaaS-ATO Memo 2013 **Interview:** Cloud Computing Assessment Discussion with Terremark 05232013				
Task: RM-8	**Evaluate the projects security and risk analysis.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 3	**Completeness:** 3 open security POAMs as of April 9. Work in progress.	3	4	12	**Moderate**
Finding Detail	The Terremark 4-Corner Report includes tracking of this issue: "CAP: Failure to meet section C.4.5, "Security Requirements", of the Statement of Work. POAMs." The POAMs have been identified in the ATO letters, and completing the milestones are considered contractual requirement that are being tracked by the Contracting Officer. However, most of the due dates have passed, and two will be past due when this report is delivered. It does not appear that these deadlines will be met.				
Potential Impact	If sensitive data is hosted and breached before the vulnerabilities are mitigated or closed, then there "may be embarrassment to CMS" or other consequences. Health plans and plan deficiency data are already being hosted by Terremark. This is commercial information requiring moderate protection.				
Recommendation	• Ensure POAMs are met by the due date and take steps to mitigate the security risk where possible. • Before hosting sensitive application data, ensure that these POAMs are closed.				
Source(s)	**CALT:**				

	doc12879 TMRK PaaS GSS FIPS-199 SYSTEM SECURITY LEVEL **GTL:** CMS Weekly Status - 4Corner - April 22, 2013				
Task: RM-9	**Verify that processes and equipment are in place to back up client and project data and files and archive them safely at appropriate intervals.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Correctness:** Asigra tool not upgraded to provide consolidated reports for cloud backups.	4	4	16	**High**
Finding Detail	Issue number 1028 on the HHS-CMS Issues Log from April 22, 2013 indicates that the Asigra tool has not been upgraded to provide consolidated reports for cloud backups. This issue has been open since December 28, 2012 with a priority of "High". During a meeting with Terremark held on May 21, 2013 it was stated that there is no defined schedule for the Asigra upgrade even though it is stated in the issue log that the upgrade to provide consolidated backup reports is slated for June 2013. Currently the only way to check the status of cloud backups is to manually log on to over 60 servers every morning.				
Potential Impact	If backups are not successful the application will be in jeopardy when servers need to be restored and backups have not been successfully created.				
Recommendation	Upgrade the Asigra software by the end of June 2013.				
Source(s)	**GTL:** CMS Weekly Status – 4Corner – April 22, 2013				
Task: RM-9		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 2	**Correctness:** Duplicate backup documents doc12881 and doc7475.	5	1	5	**Low**
Finding Detail	Artifacts doc12881 "Backup and Restore Services procedures" dated October 9, 2012 and doc7475 "ECloud Backup Process Document 05_08_2012" dated May 17, 2012 contain identical information but have different file names in CALT.				
Potential Impact	If duplicate documents exist in CALT then, confusion and time loss can occur if update is made to one of the documents and the other document is referenced by the user.				
Recommendation	Determine which document should be retained in CALT and delete the duplicate document..				
Source(s)	**CALT:** doc12881 Backup and Restore Services procedures doc7475 ECloud Backup Process Document 05_08_2012				
Task: RM-9		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 3	**Positive:** Cloud backups use an efficient tool solution.	N/A			
Finding Detail	In doc12885 "OM Manual eCAP" dated October 9, 2012, section 7.1 it states "The Asigra backup solution does not use the traditional incremental/differential/full backup types but leverages the best features of each. The initial backup is similar to a full backup and then all additional backups are similar to incremental backups as only files that have been modified are included in the nightly backup (30 versions of				

	each file are maintained). The file restore process works as if full backup were conducted each night as the system will restore the most current version (or an older version is needed) of the file(s) during a single restore process."				
Potential Impact	N/A				
Recommendation	N/A				
Source(s)	**CALT:** doc12885 OM Manual eCAP				
Task: RM-9		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 4	**Positive:** Backup site is more than 50 miles from data source as per NIST requirements.	N/A			
Finding Detail	In doc12885 "OM Manual eCAP" dated October 9, 2012, section 7.1 states that data is backed up to disk and then replicated and stored in the Culpeper and Miami data centers. The Culpeper and Miami datacenter are more than 50 miles apart from each other.				
Potential Impact	N/A				
Recommendation	N/A				
Source(s)	**CALT:** doc12885 OM Manual eCAP				
Task: RM-9		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 5	**Correctness:** Empty backup files.	5	2	10	**Moderate**
Finding Detail	It was reported at the "Daily Morning Production Call" on April 11, 2013 that some backup files were empty when needed for restore purposes causing a two day outage.				
Potential Impact	If backups are not successful, then the system is a risk when a disaster occurs and a restore is necessary to bring the system back online.				
Recommendation	Ensure backups are successful by signing onto servers to check backup status.				
Source(s)	**Meetings:** Daily Morning Production Call 05272013				
Task: RM-9		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 6	**Consistency:** Conflicting information regarding weekly backups.	5	2	10	**Moderate**
Finding Detail	Document doc12859 "CFACTS CSP4PaaS SSP" dated October 9, 2012 indicates that weekly backups are created while doc12881 "Backup and Restore Services procedures" dated October 9, 2012 indicates that incremental files are continuously created and full file backups are created only after every 10 incremental backups.				
Potential Impact	If documents contain conflicting information then, unnecessary confusion may occur when determining the frequency at which files in the cloud are backed up for restore purposes.				

Recommendation	Determine if weekly backups or only incremental back are being created and correct CALT documents doc12859 and doc12881 to indicate the true frequency of backups.				
Source(s)	**CALT:** doc12859 CFACTS CSP4PaaS SSP doc12881 Backup and Restore Services procedures				
Task: RM-12	**Verify that all system requirements have been allocated to a either a software or hardware subsystem.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Positive Finding:** The IV&V Team has found evidence that CMS bought Terremark's Service/Products that meet the SOW	N/A			
Finding Detail	In the Services.docx provided from Terremark sent to IV&V Team on Tue April 30, 2013 CMS has bought from Terremark the following Services: (1) Infrastructure -- Private Cloud – NCR (For example: Federal E-Cloud - Dedicated Cloud Service: Compute (Hybrid Network - Minimum 175Ghz/350GB RAM), etc.) (2) Infrastructure -- Shared Enterprise Cloud – MIA (For example: Federal E-Cloud - 1GHz/2GB Memory (per Ghz - Minimum 5Ghz required), etc.) (3) Infrastructure -- Colocation Services – NCR (For example: Dedicated Device Platform Fee: 208V - Effective 03U, etc.) (4) Infrastructure -- Dedicated Security Services – NCR (For example: Dedicated IDS (Including Dedicated VSS), etc.) (5) Professional Services (For example: Dedicated Support Service: Cloud Engineering, etc.) (6) Managed Services (For example: Base Cloud Managed Services (100 VMs), etc.) (7) Software (For example: CollabNet Team Forge Single ALM User (Start Date: 04/01/2013 End Date: 03/31/2014), etc.) Terremark uses Infinicenter to allow customer to access their purchased eCloud environments (referenced document: 20130426 Welcome Guide to Enterprise Cloud Federal Version LAN.docx). Also all CALT, FFE, DSH, MIDAS system are under Terremark Private Clouds. The following documents described how the software and hardware are allocated to each system. doc12880: Described all FMPS system software and hardware allocations (May be outdated since the last update date is Oct. 09, 2012) MIDAS: doc20174 has detailed allocation of software and hardware to MIDAS implementation environment. FFE: doc12381 has section 5.2.4.1 Hardware Architecture which indicate that "Figure 30 depicts the various operating systems, middle ware components, Commercial-Off-The-Shelf (COTS) products, and protocols and languages that comprise the FFE Software Architecture" CALT: doc6568 Appendix C. CALT Contingency Plan (Figure 8. CALT System Architecture) DSH: doc12925 DSH_ARC_Overview_v2.pptx (Slide 52-54 depicts the various operating systems, middle ware components, COTS products, and protocols and languages that comprise the DSH Software Architecture)				
Potential Impact	N/A				

Recommendation	N/A				
Source(s)	**CALT**: doc12880 VM Software Components doc12865 CCIIO VLAN design v2.6 doc12381 FFE_HTD doc20174 MIDAS_Operations and Maintenance Manual doc6568 CMS eCloud Contingency Plan 093011 v7 doc19387 DE-1 DE-2 MIDAS Private Cloud Impl Env Server Specifications v2.0 doc19388 MIDAS Private Cloud Test Env Server Specifications v2.0 doc19391OE-5 OE-7 MIDAS Software Tools List doc12925 DSH_ARC_Overview_v2 **GTL**: Services 20130426 Welcome Guide to Enterprise Cloud Federal Version LAN				
Task: RM-12		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 2	**Completion:** CALT Contingency Plan is missing Information.	**2**	**5**	**10**	**Moderate**
Finding Detail	The Contingency Plan is missing information. Details are provided in the Evaluation of the CALT CP document provided by MITRE. The CP has been approved but the CALT Contingency Plan has not been updated.				
Potential Impact	If the contingency plan is missing information, then the contingency plan may not be able to be executed.				
Recommendation	Update the CALT Contingency Plan.				
Source(s)	**CALT**: artf125604: CALT Security #21: Contingency Plan Missing Information CALT CP v1.1.docx (referenced in artf125604)				
Task: RM-12		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 3	**Correctness:** Miami (DR Failover site) does not have enough processors, memory, storage allocated to meet the 24/7 operating requirement in the SOW.	**4**	**5**	**20**	**High**
Finding Detail	CMS do not have disk space, memory, and processors allocated at DR Failover site. The following diagram shows The number of total processor (GHz), Processors (#VPUs), Memory (GB) and Storage (GB) on both primary and failover sites. Apparently Failover site has much less compare to primary site. CCIIO cloud resource allocations and capacity balances (referenced from CCIIO Resource Allocations by Project - ECPE Cloud 20130419.pdf)				

	Culpeper (Primary Site)	Miami (DR Failover Site)

	Processor (GHz)	Processors (#VPUs)	Memory (GB)	Storage (GB)	Processor (GHz)	Processors (#VPUs)	Memory (GB)	Storage (GB)
Current Allocations	6800	1961	14480	401280	394	133	788	33800
Capacity Factor	2	2	1	1	2	2	1	1
Potential Capacity	13600	3922	14480	401280	788	266	788	33800
Reserve Capacity Factor	0.85	0.85	0.8	0.7	0.85	0.85	0.8	0.7
Available Capacity	11560	3333	11584	280896	669.8	226	630.4	23660

During the Interview with Terremark May 23, we questioned "Why DR Failover site does not provide enough space", Terremark said that is project owner's decision.

Potential Impact

If DR Failover site does not provide enough space, lots of projects will not be able to failover to the DR site in case of fire, flooding, and earthquake happens. The production site will be unavailable.

Recommendation

- Provide the same configuration on the failover site as the primary site.
- Make processes and procedures to synchronize primary site data files with failover site data files to ensure that when primary site is lost the failover site can take over right away.

Source(s)

CALT:
doc12859 CFACTS CSP4 PaaS System Security Plan Final090412
GTL:
CCIIO Resource Allocations by Project - ECPE Cloud 20130419
OptYr2 Mod7 HHS SOW v11

Task: RM-12		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 4	**Correctness:** Multiple projects are not allocated to the DR Failover site.	**2**	**5**	**10**	**Moderate**

Finding Detail

Most of the projects in CMS do not have disk space, memory, and processors allocated at DR Failover site.
(referenced from CCIIO Resource Allocations by Project - ECPE Cloud 20130419.pdf)

CCIIO Cloud Resource Allocations by Project (as provisioned)

	Culpeper				Miami (DR Failover)			
	Virtual Machines (VMs)	Processors (#VPUs)	Memory (GB)	Storage (GB)	Virtual Machines (VMs)	Processors (#VPUs)	Memory (GB)	Storage (GB)
CALT Project Total	37	74	240	7050	6	10	18	794
CMMI Project Total	9	36	144	2240	0	0	0	0
CMSNet Project Total	3	4	28	275	0	0	0	0
DSH Project Total	142	597	1850	30420	0	0	0	0
ECWS Project Total	62	142	448	10525	0	0	0	0
EIDM Project Total	67	310	700	13540	0	0	0	0
FFE Project Total	229	544	2782	102213	0	0	0	0
HIAD Project Total	3	6	30	260	0	0	0	0
HIOS Project Total	30	39	220	4844	4	8	24	1300
LCYC Project Total	23	57	146	1745	0	0	0	0
MIDAS Project Total	70	125	317.25	14655	0	0	0	0
RBIS Project Total	54	84	456	8466	10	10	60	1984
SAS Project Total	5	12	36	1600	0	0	0	0
SERTS Project Total	13	29	46	2550	0	0	0	0
TeamMate Project Total	6	12	28	750	0	0	0	0
TEFT Project Total	22	78	156	2330	0	0	0	0
Tivoli Project Total	11	46	128	4100	0	0	0	0
TWS Project Total	8	32	120	1480	0	0	0	0
VM Clones (Temporary)	10	18	26	1630				
Development	0	0	0	0				
App Totals	804	2245	7901.25	210673	20	28	102	4078
Management	46	106	145.75	7967	4	8	14	250
Backup	0	0	0	0	2	2	2	80
Security	11	30	79.06	4237	2	8	16	740
Imaging	8	16	13.5	715	2	2	1.5	50
Admin Totals	65	152	238.31	12919	10	20	33.5	1120

Potential Impact	The DR Failover site should be a hot backup site, which means that all files in the primary site should be backup to failover over in a timely manner.
Recommendation	• Provide the same configuration on the failover site • Make processes and procedures to synchronize primary site data files with failover site data files to ensure that when primary site is lost the failover site can take over right away.
Source(s)	**CALT**: doc12859 CFACTS CSP4 PaaS System Security Plan Final090412 **GTL**: CCIIO Resource Allocations by Project - ECPE Cloud 20130419

Task: RM-12		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 5	**Accuracy:** The backup method of eCloud is inconsistent across files	2	5	10	**Moderate**
Finding Detail	According to SSP (doc12859), there should be a fully (hot) backup in Miami site. The SSP (doc12859) Page 80 -- 3.6.5 CP-6 Alternate Storage Site States:				

	"Implementation Status: In Place (Fully Satisfied) -- -- IaaS Enhancement 1 - IaaS The offsite storage facility is located at least 50 miles away from the primary site and would not be susceptible to the same hazards. Additionally, IaaS-Terremark **"hot" backup is located in Miami, Florida.** IaaS Enhancement 3 - IaaS-Terremark uses a third party, Iron Mountain, as a backup management vendor for alternate site storage. The site is a minimum of 50 miles away from the NAP of the Capital Region which reduces the likelihood that it would be impacted by the same wide-area disruption." According to Backup and Restore Services (doc12881) "1 Introduction This document provides information about the Asigra backup software and the backup process for the CCIIO ECloud. Backups occur nightly beginning at 9PM. Data is backed up to disk and then replicated and stored in the Culpeper and Miami data centers. Apparently, the SSP is saying that the backup is a hot backup and hot backup means (https://access.redhat.com/site/documentation/en-US/Red_Hat_Enterprise_Linux/4/html/Introduction_To_System_Administration/s2-disaster-recovery-sites.html) "Hot backup sites have a virtual mirror image of your current data center, with all systems configured and waiting only for the last backups of your user data from your off-site storage facility. As you can imagine, a hot backup site can often be brought up to full production in no more than a few hours." While doc12881 saying is much like cold backup (https://access.redhat.com/site/documentation/en-US/Red_Hat_Enterprise_Linux/4/html/Introduction_To_System_Administration/s2-disaster-recovery-sites.html). A cold backup site is little more than an appropriately configured space in a building. Everything required to restore service to your users must be procured and delivered to the site before the process of recovery can begin. The delay going from a cold backup site to full operation can be substantial.				
Potential Impact	If the backup method of eCloud is inconsistent across files, then the person executing the backup will not have a way to know which file is correct, causing confusion in the backup of the production environment. If it is hot backup, then there is no need for restore, since files at both primary site and DR site are in sync, so the DR site can be up promptly and may need make sure services and configuration are done correctly when the production primary site is down. While a cold backup needs to restore files from primary site and have to be copied to the DR sites, and also configuration needs to be done to make sure production system can be restored to operations. This may take several days.				
Recommendation	Review the backup and recovery procedures, and make decisions on which method should be used and update the documents to ensure files are consistent in backup/restore methodology.				
Source(s)	**CALT**: doc12859 CFACTS CSP4 PaaS System Security Plan Final090412 doc12881 Backup and Restore Services Procedures				
Task: RM-12		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 6	**Completeness:** Project: PaaS and IaaS Documents are not up-to-date in CALT	**1**	**5**	**5**	**Low**

Finding Detail	Documents in PaaS and IaaS folders are from 2012 and older. Only one file from PaaS and one file from IaaS are from 2013. For example: doc12885 OM_Manual_eCAP.doc, Chapter 3 and 4 missing details and Page 9 2012CCIIO Logical VLAN Infrastructure Presentation figure 1 is out of date (it is v1.5, doc12865 shows v 2.6)
Potential Impact	If no current documents available, the IV&V's evaluation of whether all system requirements have been allocated to a either software or hardware subsystems may not be correct, and the conclusions cannot be accurate.
Recommendation	Update Project: CMS OIS CIISG ACA Security Systems Document Submission in CALT to provide the latest documents.
Source(s)	**CALT**: doc12885 OM_Manual_eCAP doc12865 CCIIO VLAN design v2.6

2.2 CLOUD COMPUTING FINDINGS - OPERATING ENVIRONMENTS

Table 2-1 Cloud Computing Findings - Operating Environments

Task: OE-1	Evaluate new and existing system hardware configurations to determine if their performance is adequate to meet existing and proposed system requirements.	Prob (P)	Impact (I)	Risk Score (P x I)	Risk Level
Finding 1	**Verifiability**: The Capacity Plan along with supporting metrics is not available to make a determination for this task item.	**3**	**4**	**12**	**Moderate**
Finding Detail	The artifacts arising out of the Capacity Planning document [doc13247, Pg.1, Figure 1. Capacity planning process for the Cloud (i.e., Develop templates from system architecture, Stress test in cloud for point of collapse, test horizontal scale, Test forecasts)] are not available in CALT to make a determination on whether new and existing system hardware configurations and their performance are adequate to meet existing and proposed system requirements. The Capacity Planning document (Pg.3) states "…Capacity Planning, as a process for cloud, has some inherent advantages over traditional capacity planning. Unlike traditional capacity planning where procurement of assets is required to effectively load test systems, discreet testing can be conducted on cloud systems to help develop effective metrics in short periods of time. Further, different configurations and sizing of resources can be conducted to optimize the capacity plan…" Relevant metrics for the analysis will be derived from evaluating: • Service Level Agreements for the system • Performance Management • Network Management • Database Management • Application Management • Availability Management • Operations Management • Problem Management • Change Management • Other generic metrics include ▪ Compute Utilization (Generally by CPU equivalents of 1 GHz) ▪ Memory Utilization (GBs) ▪ Disk IO (Operations per second) ▪ Disk Utilization (GBs) ▪ Network IO (MBs per second)				

Potential Impact	If a workload categorization of the Cloud environment (users, data, hardware, software, SLAs, etc.) is not defined, analyzed and forecasted, then it would be difficult to fully assess whether system hardware configurations and their performance is adequate to fulfill the business need, thereby, leading to inadequate configuration issues in the Production environment.				
Recommendation	Terremark General Support System (GSS) and the Infrastructure are in an operational system status (pg.8 Center-for-Consumer-Information-and-Insurance-Oversight-TMRK_CSP4IaaS-999-SSP-08-30-2012); thus, it is particularly important that a capacity plan is in place to avert production problems. CMS and relevant contractors should carry-out a capacity planning lifecycle exercise (and provide the artifacts in CALT) to more fully address the current business requirements and also do forecasts based on projected processing requirements to meet future business needs.				
Source(s)	**CALT:** doc13247 Capacity Planning 10-17-12 doc11023 CSP4IaaSArtifactsUpdate091212 (folder) **GTL:** Services				
Task: OE-1		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 2	**Completeness**: Current hardware server configurations and related processes appear to be inadequate.	**5**	**4**	**20**	**High**
Finding Detail	Communications from daily stakeholder meetings indicate a trend of inadequate hardware server configurations and the processes involved in the configurations. A few examples of problem configurations are: 1. Downed server resources a. Citrix Installs: IDL Team is still working with URS/Terremark to resolve issue on VM servers (MIDAS Daily Scrum MOM 05212013) b. Patching and the CALT server went down (20130513 Daily Morning Production Call) 2. Backups can't intervene with the production environment (20130509 CCB IT Operational Meeting Minutes). 3. Get to IMP0 because there is a fix that affects performance (20130509 Daily Morning Production Call). 4. Deployment late last night. Smoke testing had issues; it did not pass. We are looking into how to resolve the issues. IMP0 is not functional for the QHP application (20130516 Daily Morning Production Call) 5. Resource bundle issue… usually resolved in the data layer. I don't have a handle on what the columns are. I don't believe that it is entirely the code base application (20130516 Daily Morning Production Call). The following metrics are required to estimate the capacity(doc13247): 1. Compute Utilization (Generally by CPU equivalents of 1 GHz) 2. Memory Utilization (GBs) 3. Disk IO (Operations per second) 4. Disk Utilization (GBs) 5. Network IO (MBs per second)				

	The Terremark SOW states: 1. The contractor shall provide CMS and its team access to monitoring utilities, reports, and metrics so that CMS may determine the efficiencies, costs, and needs for adjustment of the IaaS capacities that align with requirements and usage patterns of the Service [section 3.4.2 General Requirements, OptYr2 Mod 7 HHS SOW (CMS Cloud)v11].
Potential Impact	If new and existing system hardware configurations lead to system downtime for system users, then the system will not function as envisioned and may not meet the business requirements.
Recommendation	Review the existing system capacity (referencing the items listed below) to derive a hardware solution which meets current and projected system requirements: 1. Cloud Demand/Capacity 2. Resource Provisioning Management 3. Cloud Operations 4. Availability Management 5. Incident Management 6. Problem Management 7. Access Management 8. Event Management
Source(s)	**CALT:** doc8179 Provisioning Process Legend doc8175 Cloud Processes doc8177 Platform Delivery Process v02 **GTL:** OptYr2 Mod 7 HHS SOW (CMS Cloud)v11 CMS Weekly Status - 4Corner - April 22, 2013 **Meetings:** MIDAS Daily Scrum MOM 05212013 CCB IT Operational Meeting Minutes 05092013 Daily Morning Production Call 05092013 Daily Morning Production Call 05132013 Daily Morning Production Call 05162013

Task: OE-1		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 3	**Verifiability:** Artifacts needed to conduct a thorough review of cloud services are only available in piecemeal fashion in CALT.	**4**	**3**	**12**	**Moderate**
Finding Detail	Artifacts in the 'Output' column below are needed to determine whether new and existing system hardware configurations and their performance is adequate to meet existing and proposed system requirements; access to Terremark's Infinicenter will provide some of the artifacts needed for analysis; Additionally, artifacts provided through the Nagios & Groundwork tools are also required for this assessment				

task item.

doc8175 Cloud_Processes, [Processes] tab:

Management Area	Process	Output
Cloud Demand/Capacity	Resource provisioning management	Executive dashboard report
Cloud Operations	Availability management	Executive dashboard report
	Incident management	Executive dashboard report
	Problem management	Executive dashboard Report
	Access management	Manager's report
	Event management	Manager's report

Potential Impact: If necessary artifacts are not made available to IV&V to perform an assessment on the cloud infrastructure, then a review of the infrastructure environment will not be provided to CMS management and deficiencies in the system may be present which are not addressed.

Recommendation: Provide IV&V with the necessary artifacts and tools access to enable a review of this task item.

Source(s):
CALT:
doc11023 CSP4IaaSArtifactsUpdate091212 (folder)
doc12949 PaaS Release Management Plan
doc8175 Cloud_Processes
doc13247 Capacity Planning 10-17-12
GTL:
[1]CCIIO Resource Allocations by Project - ECPE Cloud 20130419
IVV Questionnaire_Terremark Responses May 20 2013
CLOUD GAP Analysis 20130521
Interview:
Cloud Computing Assessment Discussion with Terremark 4/30/2013
IV&V CALT Demo Interview 05132013
Cloud Computing Assessment Discussion with Terremark 5/23/2013

Task: OE-2	Determine if hardware is compatible with other federal existing processing environment, if it is maintainable, and if it is easily upgradeable. This evaluation	Prob (P)	Impact (I)	Risk Score (P x I)	Risk Level

	will include, but is not limited to CPUs and other processors, memory, network connections and bandwidth, communication controllers, telecommunications systems (LAN/WAN), terminals, printers and storage devices.				
Finding 1	**Process Deviation**: The current Cloud infrastructure (i.e., hardware) has deviated from the defined and approved security policy as detailed in the Terremark SOW.	**5**	**5**	**25**	**High**
Finding Detail	The FMPS infrastructure is not currently FISMA compliant as called for in the Terremark SOW. Excerpts taken from '4Corner - April 22, 2013' report below indicate FISMA non-compliance issues: • Pg.2, CMS Weekly Status - 4Corner - April 22, 2013: **HHS-CMS Issues Log** The Terremark SOW (OptYr2 Mod 7 HHS SOW (CMS Cloud v11, C3. Objective, details the FISMA requirement: The tools required by CMS to manage the Exchange program are, 1) a state of the art, FISMA compliant cloud-based infrastructure and platform that can dynamically scale as needed; 2) a secured cloud-based ALM that functions as a component of a Platform as-a-Service (PaaS); and 3) a secure cloud application platform for workflow management, ticketing management, and documentation and application delivery platform which will increase the overall PaaS capability.				
Potential Impact	If the FEPS infrastructure is not FISMA-compliant (i.e., deviation from stated policies and contractual agreements), then the system may not be secure and uncorrected vulnerabilities may be exploited.				
Recommendation	CMS should mandate that the Cloud infrastructure become FISMA compliant a.s.a.p.				
Source(s)	**GTL:** OptYr2 Mod 7 HHS SOW (CMS Cloud)v11				

No.	Priority	Description	Owner	Date Opened	Resolution /Notes	Date Closed
1028	High	CAP: Failure to meet contractual requirement: Ensure the services provided are compliant with the Federal Information Security Management Act (FISMA). Backups not completing. Requested visibility to backup job notifications.	Paul Weiss	Dec 28	As of March 1 all backups reported functioning as expected. Ver. 12 of Asigra stated to provide consolidated backup reports. – eta June 2013.	
1029	High	CAP: Failure to meet section C.4.5, "Security Requirements", of the Statement of Work. POA&Ms – 6 remaining as of March 15.	Paul Weiss	Dec 28	3 closed and 3 open as of April 9. Work in progress.	
1030	High	CAP: Failure to meet section C.4.5 of the Statement of Work requiring Terremark to provide a FISMA Compliance Solution for continuous monitoring (nCircle) for the network security requirements mandated by FISMA, and the Department of Health and Human Services.	Paul Weiss	Dec 28	Re-architecture of nCircle scanning in process. Stakeholders: Tom Schankweiler and Mike Fluharty.	
1031	High	CAP: Failure to satisfy Section 508 legal requirements.	Paul Weiss	Dec 28	Expect to be completed by April 30.	

	CMS Weekly Status - 4Corner - April 22, 2013 CMS Weekly Status - 4Corner - May 20, 2013 -REV A				
Task: OE-2		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 2	**Verifiability:** Artifacts supporting adherence to the CMS TRA – Virtualization Supplement was not found in CALT.	**4**	**3**	**12**	**Moderate**
Finding Detail	Evidence pertaining to infrastructure cloud compliance to CMS' TRA was not found; the document 'CMS TRA – Virtualization Supplement' (pg.1) states: • This document defines the Virtualization guidelines and standards for the CMS Production Environments. Once the Agency promulgates these standards, this document should assist all Agency contractors in sustaining the three critical technical objectives in support of CMS' health care mission: (1) move CMS Production workloads efficiently, (2) provide appropriate and sufficient disaster recovery capability, and (3) facilitate the migration and transition of CMS Business Owner applications into new production environments. Variations to the TRA Virtualization standards require consensus from all specified contractor stakeholders and explicit approval from CMS' technical and executive-level management.				
Potential Impact	If the evolving cloud infrastructure is not CMS TRA compliant, then the delivered system may not fulfill the strategic goals of the organization.				
Recommendation	CMS should require that evidence be provided on whether the cloud is CMS TRA compliant.				
Source(s)	**CALT:** doc11023 CSP4IaaSArtifactsUpdate091212 (folder) doc12975 CMS eCloud Governance – Contingency Plan doc10998 PaaS C&A Artifacts 2 **GTL:** CMS TRA Virtualization Supp v 1 1_07282010				
Task: OE-2		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 3	**Positive Finding:** The FMPS Infrastructure solution appears to be maintainable and upgradeable.	N/A			
Finding Detail	The FMPS Solution Architecture – Key Design Principles, (Slide 4, FFE_ArchitecturalDiagrams) depict an environment that is: • Open (SOA and Component based, Open-standards based interfaces) • Scalable (End-to-end scalability to support 21 million enrollments in FFE and expanding to 41 million enrollments) • Simple (Hide complexity of complex integrations using well-defined interfaces and patterns, Simplify entire solution lifecycle - development, operations, and maintenance) • Secure (Multi-zone architecture to protect personal health, identity, and financial data, infrastructure, and communications) The additional artifacts listed below, provides further evidence that the cloud infrastructure is maintainable and upgradeable.				
Potential Impact	N/A				

Recommendation	N/A				
Source(s)	**CALT:** doc6148 MIDAS Server Specifications v0.7 doc12865 CCIIO VLAN design doc10998 PaaS C&A Artifacts 2 doc11023 CSP4IaaSArtifactsUpdate091212 (folder) **GTL:** CMS TRA Virtualization Supp v 1 1_07282010 VM Software Components CCIIO Enterprise Cloud Infrastructure 3-Zone Architecture with Defined Regions CCIIO Resource Allocations by Project - ECPE Cloud 20130419				
Task: OE-3	**Evaluate current and projected vendor support of the hardware.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Verifiability:** Unable to evaluate the Hardware vendor support.	3	2	6	**Moderate**
Finding Detail	Tab "CSP4IaaS Hardware" in the document "VM Software and Hardware Components" mentions about the Hardware specifications as well as the Hardware but could not find any evidence of Hardware vendor support.				
Potential Impact	Non availability of hardware vendor support documents can impact future timely support and resolution.				
Recommendation	Hardware vendor support documents should be readily available and accessible to review in CALT.				
Source(s)	**GTL:** VM Software and Hardware Components provided by Terremark				
Task: OE-3		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 2	**Positive Finding:** Monthly scan reports for Hardware and Services are supported by the vendor.	N/A			
Finding Detail	1. IaaS contingency plan and Contingency plan contact list is documented in the document "Center-for-Consumer-Information-and-Insurance-Oversight-TMRK_CSP4IaaS-CP-09062012" 2. Slide 10,11,13 of the "doc10229-SCA and Cloud GSS 08102012-2" show that there are security services & Monitoring controls of the Hardware supported by the vendor. 3. Document "POAM Scan results IaaS.docx" explains the rating system for the monthly scans results provided by Terremark to CMS. 4. "Services.docx" – Contains all the services provided by Terremark.				
Potential Impact	N/A				
Recommendation	N/A				
Source(s)	**CALT:** doc10229 SCA and Cloud GSS 08102012-2				

	doc10998 PaaS C&A Artifacts 2				
Task: OE-4	**Evaluate new and existing system software to determine if its capabilities are adequate to meet existing and proposed system requirements.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Positive Finding:** System software support services provided by Terremark are detailed in the Services.docx.	N/A			
Finding Detail	All the software services provided by Terremark are listed under CLIN '8' in the "services.docx" document and are still valid. Software support Services listed in the document "services.docx" is adequate in meeting the existing system requirements. They are currently valid until end of march'2014.				
Potential Impact	N/A				
Recommendation	Make sure the validity of the support services is not expired.				
Source(s)	**GTL**: Services				
Task: OE-4		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 2	**Completeness:** No evidence of Integration Management artifacts was found to evaluate the system software integration process.	3	4	12	**Moderate**
Finding Detail	Following is stated in section C.4.2 "General Requirements" of the Terremark- SOW. • Provide Integration Support Services to coordinate the configuration, staging and deployment of system components between the CMS's IaaS and the PaaS solutions. Support will be provided to maintain configuration management baselines and system security profiles. Specific support under this task includes Software Configuration Management and Integration Management. Although, IV&V team was able to find the Configuration Management plan (CALT: doc30440), we did not find any documents for the Integration Management.				
Potential Impact	If there is no Integration Management plan, then it impacts IV&V team ability to evaluate that the software integration processes/procedures being followed as stated in the Terremark SOW.				
Recommendation	Integration Management plan must be readily available to evaluate the software Integration process. Integration management is a critical aspect of large-scale information technology project execution, given the many interlocking activities and work streams that must effectively come together to achieve project success.				
Source(s)	**CALT**: doc30440 Configuration_Management_Plan_v1.2 09062012 **GTL:** OptYr2 Mod 7 HHS SOW (CMS Cloud)v11				
Task: OE-5	**Determine if the software is compatible with other federal existing hardware**	**Prob**	**Impact**	**Risk Score**	**Risk Level**

	and software environment, if it is maintainable, and if it is easily upgradeable. This evaluation will include, but is not limited to, operating systems, middleware, and network software including communications and file-sharing protocols.	**(P)**	**(I)**	**(P x I)**	
Finding 1	**Positive Finding**: Evidence was found that the development software is maintainable, easily upgradeable, and compatible with CMS's existing environment and is following the Federal Enterprise Architecture.	N/A			
Finding Detail	Operational and infrastructure documentation found in CALT supports adherence to the Technical Reference Architecture and associated supplement documentation. Functional system operations including the operating environment are identified in the PM_R3S9_EHB_OpsMaintManual (doc12461). An operational analysis including impacts is discussed in the FFE_HTD (doc12381).				
Potential Impact	N/A				
Recommendation	Continue to assess this area as operating environment needs expand.				
Source(s)	**CALT:** doc12461 PM_R3S9_EHB_OpsMaintManual doc12381 FFE_HTD, doc11023 - CSP4IaaS C&A Artifacts Update 091212 doc2475 Exchange Reference Architecture Foundation Guide doc2744 CMS TRA Web Services Suppl_Draft V06_052311 doc12878 TMRK CSP4PaaS RA Final 09062012 doc12885 OM_Manual_eCAP doc12881 Backup and Restore Services, doc12873-Enterprise Cloud Roles and Responsibilities Identification and Definition v 1 0 doc12864 CCIIO PaaSCloud VLAN Assignments (1) doc12865 CCIIO VLAN design v2.6, doc12866-CCIIO VLAN Shared Services v2.5 **Standards:** CMS Federal Enterprise Architecture (FEA), CMS Technical Reference Architecture (TRA) CMS Technical Reference Architecture – Private and Community Cloud IaaS and PaaS Infrastructure Supplement.				
Task: OE-5		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 2	**Positive Finding**: Evidence was found that the software and configuration used is scalable, industry-proven and in accordance with internal standards.	N/A			
Finding Detail	Evidence of an Infrastructure as a Service (IaaS) platform that scales to support collaborative development efforts and production and industry-proven, secure, and scalable Cloud based Platform as a Service (PaaS) can be found in Doc13102 - Platform delivery process, doc12851 Configuration Management Plan, CMS Federal Enterprise Architecture. There are a number of standards and best practices being followed, which makes it compatible with other Federal HW/SW environments. (doc12381).				
Potential Impact	N/A				

Recommendation	Continue to assess compliance against set standards as part of reviews and annual attestation and approval process.				
Source(s)	**CALT:** doc12851 CALT CFACTS CM Plan doc12381 FFE_HTD, doc11023 - CSP4IaaS C&A Artifacts Update 091212 doc13102 Platform delivery process doc28366 IaaS FY2013 Attestation Input **Standards:** CMS Federal Enterprise Architecture (FEA), CMS Technical Reference Architecture (TRA) CMS Technical Reference Architecture – Private and Community Cloud IaaS and PaaS Infrastructure Supplement. **Interview:** Cloud Computing Assessment Discussion with Terremark 5/21/2013 Cloud Computing Assessment Discussion with Terremark 5/23/2013				
Task: OE-5		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 3	**Consistency:** Software list is inconsistent amongst several documents in CALT.	**3**	**1**	**3**	**Low**
Finding Detail	There are a couple of differences in the software list between the software inventory document doc12880 and the Technical Design document doc12381. As an example, Informatica is listed in doc1281 but not in doc12880.				
Potential Impact	If the listed software is inconsistent between documents, then this could cause confusion as to what is really available in the environment.				
Recommendation	Review and update documents to sync up list of software installed and available in the environment.				
Source(s)	**CALT:** doc12880 PaaS VM Software Components doc12381 FFE_HTD, doc11023 - CSP4IaaS C&A Artifacts Update 091212				
Task: OE-6	**Current and projected vendor support of the software will also be evaluated.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Positive Finding**: Review of evidence found that the software installed in the environment is from established and well-known software companies.	N/A			
Finding Detail	The list of software components as evidenced in doc12880 and doc12381 is from well-established companies will be around for a while to provide support. Another positive note is that there is a list of approved applications for use to support the Terremark infrastructure in customer requirements as evidenced in doc11023. Additionally, IV&V team visited most of these vendor sites as well as analyzed internal issues and incidents logs looking for issues and trends and found no evidence of abnormalities.				
Potential Impact	N/A				
Recommendation	Create and upload a document in CALT listing all software managed by Terremark or partners.				
Source(s)	**CALT**: doc12880 PaaS VM Software Components				

	doc12381 FFE_HTD doc11023 CSP4IaaS C&A Artifacts Update 091212 doc13090 Provisioning Process Legend				
Task: OE-6		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 2	**Verifiability:** Unable to verify vendor software support	**4**	**3**	**12**	**Moderate**
Finding Detail	There was no evidence located in CALT on SLA or any other type of documentation detailing vendor software support. We found evidence of list of installed software and approved applications but found no evidence of the level of vendor support. Here's a partial list of some of the software: Oracle 11gR2, SAS Windows Clients 9.3, Citrix XenApp Server 6.5, Citrix Data Collector 6.5, SQL Server 2008 R2 SP1, MarkLogic 5.0,2, Apache 2.2.15, Drupal 7.12, Sugar CRM 6.3.1, Informatica, Cognos etc.				
Potential Impact	If vendor software support is not readily documented and available, then this could impact timely support and resolution on software issues.				
Recommendation	Vendor software support documentation and SLA should be made available in a centralized location and process put in place to review annually.				
Source(s)	**CALT:** doc12880 PaaS VM Software Components doc12381 FFE_HTD doc11023 CSP4IaaS C&A Artifacts Update 091212				
Task: OE-10	**Evaluate the existing processing capacity of the system and verify that it is adequate for current statewide needs for both batch and on-line processing.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Positive Finding:** Evidence found that Terremark uses a portal called Infinicenter to generate capacity reports and provide the report to CMS.	N/A			
Finding Detail	Bandwidth report sample is included in the 4-corner report. 4-corner report shows aggregate purchased, allocated and utilized VMs, memory and storage per resource pool. The eCAP team uses Nagios (open-source network and system monitoring platform) to monitor VMs in the cloud environment in order to ensure that disk, RAM and CPU resources are within set limits and to ensure that customer services are functioning properly.				
Potential Impact	N/A				
Recommendation	N/A				
Source(s)	**CALT:** doc12885 OM Manual eCAP **GTL:** CMS Weekly Status - 4Corner - April 22, 2013 CMS Weekly Status - 4Corner - May 20, 2013 -REV A				
Task: OE-10		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**

Finding 2	**Completeness:** Input elements used to evaluate existing capacity are not identified in doc8175 (Cloud Processes).	**3**	**4**	**12**	**Moderate**

Finding Detail	Details on FMPS existing and proposed system requirements as outlined in doc8175 Cloud Processes are missing.
	
	The details of the input elements specified in the capacity planning document doc13247 are missing such as:
	• Application modeling results
	  ○ Expected Scenarios, Use Cases/Scenarios
	• Current Operations Metrics
	  ○ User loads per hour
	  ○ Interactions per hour
	  ○ System metrics (ideally by node)
	  ○ Current allocated capacity
	• Operation Forecasts
	  ○ Trends of median and maximum users over time
	  ○ Projections of users
	  ○ Cyclical nature of system utilization process
	• Cloud Demand/Capacity
	• Resource Provisioning Management
	• Cloud Operations
	• Availability Management
	• Incident Management				

Potential impact	If proper capacity planning is not done then it will affect system performance				
Recommendation	Provide the details of all the inputs used for capacity planning In a document.				
Source(s)	**CALT:** doc11023 CSP4IaaSArtifactsUpdate091212 (folder) doc12949 PaaS Release Management Plan doc8175 Cloud_Processes doc13247 Capacity Planning 10-17-12 **GTL:** [1]CCIIO Resource Allocations by Project - ECPE Cloud 20130419 **Interview:** IV&V CALT Demo Interview 05132013				
Task: OE-10		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 4	**Correctness:** The existing capacity planning is not adequate.	**4**	**4**	**16**	**High**
Finding Detail	Existing capacity of the system is not adequate from the 4 corner chart. It was found there is a shortage of VMs ad processors in the report of				

	May 2013. A cloud that cannot fulfill requests effectively will not deliver on the promise of improved speed to systems deployment. To successfully manage a cloud computing environment, it is critical to identify the optimal amount of cloud infrastructure required to meet the anticipated needs of end users. If there are too few computing resources, requests from users will either have to wait for resources to free up, or will be rejected until more hardware is added to the environment. Many incidents of capacity issues with warning about disk space used from CALT (artf135295,artf135296,artf135594) And daily morning production call meeting (05/28/13). The 4corner report shows that the Bandwidth usage increased drastically from April, 2013(57.7Mbps, 3.9 TB) to May2013(342Mbps				
Potential impact	If the existing capacity planning of the system is not adequate then a shortage of system resources will lead to performance issues and system failure.				
Recommendation	CMS should review the existing system capacity and utilize system metrics to forecast future capacity requirements.				
Source(s)	**CALT**: doc12975 CMS eCloud Governance – Contingency Plan artf135295,artf135296,artf135594 **GTL:** CMS Weekly Status - 4Corner - May 20, 2013 -REV A **Meetings**: Daily Morning Production Call 05282013				
Task: OE-10		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 5	**Process Deviation/Consistency:** Inputs required for capacity planning are not consistent.	**4**	**3**	**12**	**Moderate**
Finding Detail	IV&V Team has found that numbers of users have been specified in many different documents, but there is no single document to estimate the capacity based on the input metrics as explained in the capacity planning document.				
Potential impact	Shortage of system resources will lead to performance issues ad system failure.				
Recommendation	Provide a single document for capacity planning including all the input metrics like the number of users. Transactions etc., Provide the formula or standards applied to estimate the capacity in the document.				
Source(s)	**CALT**: doc12975 CMS eCloud Governance – Contingency Plan doc11232 FFE_ArchitecturalDiagrams_Internal doc12461 PM_R3S9_EHB_OpsMaintManua doc5749 MIDAS System Design Document doc26320 DSH_IMP_OMM				

	doc26316 DSH_PLAN_CONOP				
Task: OE-11	**Evaluate the historic availability and reliability of the system including the frequency and criticality of system failure.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Verifiability**: Unable to review evidence on the individual server usage statistics like web server usage statistics.	**2**	**5**	**10**	**Moderate**
Finding Detail	There is evidence on total system availability, business application availability, system usage and Help Desk call volume by severity; however, no evidence was available for review on the web server usage statistics. Even though the Reports on identifying SLA performance per month are available through the Infinicenter, access to Infinicenter to look into these performance reports was not available.				
Potential Impact	If there is no report on how the individual server usage statistics like web, application servers, and then it would be difficult at given time to address the performance issues and recommends improvements.				
Recommendation	Make reports on individual usage statistics available in CALT.				
Source(s)	**CALT**: doc12975 CMS eCloud Governance – Contingency Plan **Meetings:** Daily Morning Production Call 05092013 Daily Morning Production Call 05102013 Daily Morning Production Call 05132013				
Task: OE-11		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 2	**Positive Finding:** eCloud Governance Contingency Plan is in place	**N/A**			
Finding Detail	Contingency plan is in place for the eCloud and explained in detailed in doc12975 CMS eCloud Governance – Contingency Plan				
Potential Impact	N/A				
Recommendation	N/A				
Source(s)	**CALT**: doc12975 CMS eCloud Governance – Contingency Plan				
Task: OE-12	**Evaluate the results of any volume testing or stress testing.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Verifiability:** No evidence was found of any test cases on volume testing or stress testing and its testing results in CALT	**2**	**2**	**4**	**Low**
Finding Detail	No evidence in CALT of Cloud computing documentation for any Volume or Stress testing.				
Potential Impact	If there is no Volume or Stress testing results available, then it will be difficult at any given time to address the performance issues and recommend improvements.				
Recommendation	Volume or Stress testing schedules need to be more visible to stakeholders and testing results uploaded into CALT.				

Source(s)	**GTL**: CLOUD GAP Analysis 20130521 CMS Weekly Status - 4Corner - April 22, 2013				
Task: OE-12		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 2	**Verifiability:** No evidence was found for any test cases on performance testing and its testing results in CALT	**2**	**2**	**4**	**Low**
Finding Detail	Performance testing is done per application. Terremark staff has participated in these as requested by the app owner and/or CMS. During these tests, Terremark and URS provide reports on network, storage, VMware, and VM as requested by the app owner and/or CMS. There is no standard report at this time. No evidence in CALT of Cloud computing documentation for this task area. Only evidence is the request made by CMS colo cage. 1015 High Access to technical resource who can provide reports within 30 minutes of request Henry Chao Mar 15 Provided performance testing and go live support as requested. 4/2/2013				
Potential Impact	If there is no Performance testing results are available, then it will be difficult at given time to address the performance issues and recommends improvements				
Recommendation	Performance testing schedules need to be more visible to stakeholders and testing results uploaded into CALT.				
Source(s)	**GTL**: CMS Weekly Status - 4Corner - April 22, 2013				
Task: OE-13	**Evaluate any existing measurement and capacity planning program and will evaluate the system's capacity to support future growth.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Positive Finding:** Terremark provides a portal called Infinicenter to configure and manage resources, monitor the resources and to generate historic reports.	N/A			
Finding Detail	Within the enterprise cloud, Terremark has integrated a web portal called Infinicenter to allow for rapid configuration and management of computing resources. Through this web portal, CMS and the URS OM team have a continuous view of all resources via dynamic, real-time reporting. The portal provides the ability to view the availability and health of the computing resources at both the executive and detailed operational levels. The console also enables historical data views to trend resource utilization, supporting a customer's efforts to proactively manage capacity. Access to Infinicenter is controlled by the URS PM. The URS PM identifies the URS personnel whose roles require access, authorizes the appropriate level of access, and makes a request to the InfiniCenter administrator.				
Potential Impact	N/A				
Recommendation	N/A				
Source(s)	**CALT:** doc12885 OM Manual eCAP doc13247 Capacity Planning 10-17-12				

	doc8177 Platform Delivery Process v02				
Task: OE-13		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 2	**Correctness:** The capacity planning process (doc13247) does not specify how the capacity is estimated and the formula to calculate the capacity/resources required	3	3	9	**Moderate**
Finding Detail	IV&V team found the capacity planning process(doc13247) does not specify how the capacity is estimated and the formula to calculate the capacity/resources required				
Potential Impact	If proper capacity planning is not done then it will affect system performance. Planning for sufficient availability is necessary to avoid system collapse as load increases.				
Recommendation	Document the capacity planning program used and the metrics used. Document how the resource allocation is determined.				
Source(s)	**CALT:** doc8179 Provisioning Process Legend doc13247Capacity Planning 10-17-12 doc8177 Platform Delivery Process v02				
Task: OE-13		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 3	**Verifiability:** The system's capacity to support future growth cannot be verified.	4	5	20	**High**
Finding Detail	The system's capacity to support future growth cannot be verified. There is no evidence to verify that the future demand of the system was estimated from the existing trends. There is no report in Infinicenter that shows projected growth in demand. Benchmarks can be provided through performance testing. Performance testing is scheduled in the testing playbook, but there is no evidence in CALT of a performance test plan or performance test procedures.				
Potential Impact	If proper capacity planning and performance testing are not completed then the private cloud environment may not be able to sustain the anticipated user base when the system is fully implemented				

Recommendation	IV&V team needs access to the Infinicenter. Terremark need to provide historical sample reports from Infinicenter. Performance testing goals need to be identified.
	▪ Identify performance goals and business goals
	  ○ Define operational profiles and load definitions
	  ○ Understand and select the various types of performance tests
	  ○ Define and select appropriate measurements
	▪ Infrastructure and Architecture – accessing infrastructure issues
	  ○ What must be part of the test?
	  ○ Target platform and systems
	  ○ Network configuration
	  ○ Scalability and extrapolation (inferentially derive… based upon known facts)				

Source(s)	**CALT:**				

	doc6148 MIDAS Server Specifications v0.7 doc11232 FFE_ArchitecturalDiagrams_Internal doc11023 CSP4IaaSArtifactsUpdate091212 (folder) **GTL**: CMS TRA Virtualization Supp v 1 1_07282010 VM Software Components				
Task: OE-13		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 4	**Completeness**: Terremark Infinicenter is used for capacity management. But it is not clear how the future growth is estimated.	3	3	9	**Moderate**
Finding Detail	Terremark Infinicenter is used for capacity management. But it is not clear how the future growth is estimated and steps to handle future growth. Infinicenter report only shows the processor, memory and storage trend for the past but there is no tool to Project future capacity growth. As per the Terremark SOW: The contractor shall provide proven, stable, and secured technologies: • Capable of projecting capacity growth based on forecasting and trending No evidence from the reports generated using Infinicenter that it is capable of projecting future capacity growth based on forecasting and trending.				
Potential Impact	If planning for sufficient availability is not conducted then the system will collapse as load increases.				
Recommendation	Document the model used for forecasting the future demand and methods to differentiate the trend from spikes in demand and how the Infinicenter will handle any spike or rise in demand.				
Source(s)	**CALT:** doc8179 Provisioning Process Legend doc13247 Capacity Planning 10-17-12 doc8177 Platform Delivery Process v02 **GTL:** OptYr2 Mod7 HHS SOW v11				
Task: OE-13		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 5	**Completeness:** No evidence of auto-scaling feature to meet the change in required capacity dynamically.	5	2	10	**Moderate**
Finding Detail	No evidence of auto-scaling feature to meet the change in required capacity dynamically. With Auto Scaling, you can ensure that the number of virtual machines you're using increases seamlessly during demand spikes to maintain performance, and decreases automatically during demand lulls.				
Potential Impact	If auto scaling features are available and not used then it will impact High Availability and resources have to be provisioned in advance to				

	meet the demand.
Recommendation	Clarify if auto-scaling can be enabled or not.
Source(s)	**CALT:** doc8179 Provisioning Process Legend doc13247 Capacity Planning 10-17-12 doc8177 Platform Delivery Process v02

2.3 CLOUD COMPUTING FINDINGS - SYSTEM AND ACCEPTANCE TEST

Table 2-3 Cloud Computing Findings - System and Acceptance Test

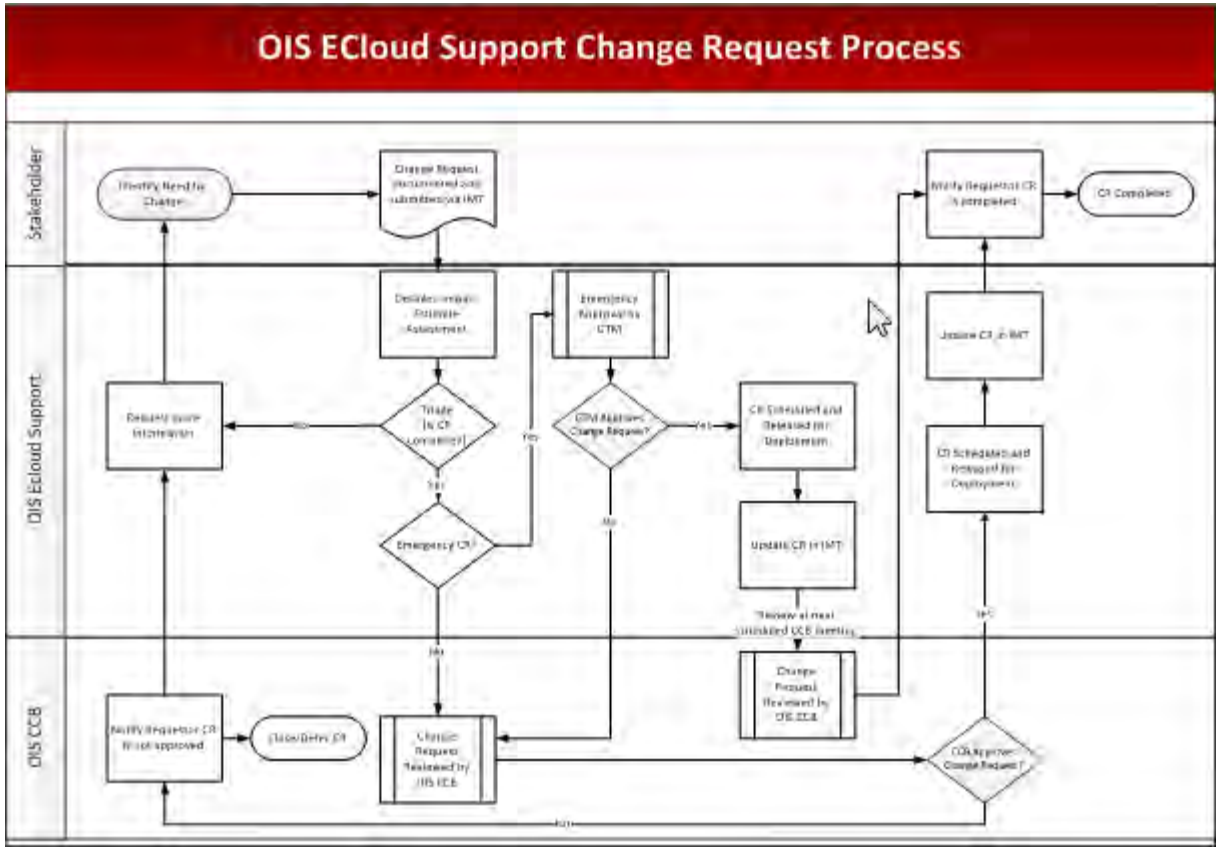
Task: ST-11	**Acceptance procedures and acceptance criteria for each product must be defined, reviewed, and approved prior to test and the results of the test must be documented. Acceptance procedures must also address the process by which any software product that does not pass acceptance testing will be corrected.**	**Prob. (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Positive Finding:** Patch testing procedure are documented in Patch and Vulnerability Management Procedure	**N/A**			
Finding Detail	The Patch and Vulnerability Management Procedure has sections that address the approach, method and responsibility for testing and acceptance of patches.				
Potential Impact	N/A				
Recommendation	N/A				
Source(s)	**CALT:** doc12886 Patch and Vulnerability Management Procedure doc12885 OM_Manual_eCAP				
Task: ST-11		**Prob. (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 2	**Positive Finding:** Recovery testing is documented in the Contingency Planning documents	**N/A**			
Finding Detail	Recovery testing after backup is part of the Backup and restore procedures				
Potential Impact	N/A				
Recommendation	N/A				
Source(s)	**CALT:** doc12881 Backup and Restore Services Procedures doc12885 OM_Manual_eCAP				
Task: ST-11		**Prob. (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 3	**Positive Finding:** Disaster Recovery testing is documented in the Contingency Planning documents	**N/A**			

Finding Detail	Testing required for disaster recovery is identified in the Contingency Plan				
Potential Impact	N/A				
Recommendation	N/A				
Source(s)	**CALT:** doc6568 CMS eCloud Contingency Plan 093011 v7 doc12885 OM_Manual_eCAP				
Task: ST-15	**Review and evaluate implementation plan.**	**Prob. (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Positive Finding:** Implementation process and procedures are folded into the various plans for Terremark operations	**N/A**			
Finding Detail	Implementation of services is identified in the Terremark service plans				
Potential Impact	N/A				
Recommendation	N/A				
Source(s)	**CALT:** doc30440 Configuration_Management_Plan_v1.2 09062012 doc12949 PaaS Release Management Plan doc6568 CMS eCloud Contingency Plan 093011 v7 doc12885 OM_Manual_eCAP				

2.4 CLOUD COMPUTING FINDINGS - OPERATIONS OVERSIGHT

Table 2-4 Cloud Computing Findings - Operations Oversight

Task: OO-1	Evaluate CMS's change request processes.	Prob (P)	Impact (I)	Risk Score (P x I)	Risk Level
Finding 1	**Positive Finding:** There is evidence and documentation of an effective change request process and defect tracking processes for eCloud.	N/A			
Finding Detail	In CALT, there is a project called CMS OIS ECloud Support. This project supports the CMS change requests and defect tracking processes. From tracker in this project, users can make the following requests: 1. VM Service Request, 2. CALT Change Request, 3. Outage Request, 4. Infrastructure Change Request, 5. Report Request, Incidents, 6. Service Requests, 7. track CALT Migration Issues , 8. track Defects, 9. System Access Request There is a Change Management Plan (CMP, doc12950) that identifies the Change Control Board (CCB) -- Technical and Business. ECloud change requests are addressed in the IT CCB meetings. The CMP is in CALT. CALT will be used as the issue management tool (IMT). CALT contains folders for agendas and meeting minutes for each type of CCB. However, Change Request (CR) tracking and CCB materials has been moved to Remedy, which is likely to reduce stakeholder access to and collaboration on these items. There is CCB IT Operational Meeting every week for CMS/OIG. The purpose of this meeting is to review and adjudicate (approve or reject/escalate) Change Requests (CR's) to base-lined items that significantly impact IT scope, schedule, or cost and affect one or more business areas.				
Potential Impact	N/A				
Recommendation	N/A				
Source(s)	**CALT**: doc12950 PaaS Change Management Plan doc12873 Enterprise Cloud Roles and Responsibilities Identification and Definition v 1 0 doc12862 Incident Management Plan_v.7				

	doc12885 OM_Manual_eCAP.doc				
Task: OO-1		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 2	**Correctness:** The Change Management Plan doesn't define a process to verify a change request has been implemented.	**3**	**4**	**12**	**Moderate**
Finding Detail	In page 7 of doc12950 of Change Request Process, between the process of "CR Scheduled and Released for Deployment" and "Update CR in IMT", the "Verify Deployment" should be added.  				
Potential Impact	If no verify deployment process is defined, then deployment may occur without the change request being implemented. The production				

	quality is in jeopardy				
Recommendation	Update all the documents that related to the change management, to define the verify deployment process, and have a role or personnel to execute this process.				
Source(s)	**CALT:** doc12950 PaaS Change Management Plan				
Task: OO-2	**Evaluate implementation of the process activities and request volumes to determine if processes are effective and are being followed.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Positive Finding:** CMS is implementing a private/community[1] Cloud Computing environment (eCloud).	N/A			
Finding Detail	The Centers for Medicare & Medicaid Services (CMS) is implementing a private/community[2] Cloud Computing environment (eCloud) for enabling convenient, on-demand network access to a shared pool of configurable computing resources. The procedures apply to eCAP Support personnel developing or providing services to support operations and maintenance in the CMS e-Cloud Applications Platform (PaaS). They are effective throughout the lifespan of the contract. As implementation and configuration requirements are provided by Terremark, Collabnet, CMS and other stakeholders, URS performs in a lead role to implement and manage the specified cloud infrastructure. Ongoing operations and maintenance activities include enforcement of cloud deployment policies, network and system administration activities, and maintaining the security of the environment.				
Potential Impact	N/A				
Recommendation	N/A				
Source(s)	**CALT:** doc12885 OM Manual eCAP				
Task: OO-2		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 2	**Consistency:** Multiple artifacts in CALT under CMS OIS ECloud Support are not implemented in accordance with the SLA.	4	5	20	**High**
Finding Detail	Based on the evaluation of project called CMS OIS ECloud Support in CALT, there is inconsistency upon implementation of requests, some are implemented on time, and some are not. According to the meeting minutes of IV&V with Terremark on May 13, there is a question and answer below. Q: Are there timeline/SLA for completing requests? A: requests are completed based on priority approved by CMS. CMS wanted to be able to prioritize regardless of when the requests came				

[1] For detailed definition, see *CMS Cloud Computing Standard,* CMS Office of the Chief Information Security Officer, Risk Management Handbook Volume III, Version 1.0, May 3, 2011

[2] For detailed definition, see *CMS Cloud Computing Standard,* CMS Office of the Chief Information Security Officer, Risk Management Handbook Volume III, Version 1.0, May 3, 2011

through.

- Terremark is capable of delivering 8 systems a day.
- Normal process is to complete a request in 3 days after CMS approval.
- Could build new server in a few hours if necessary under an emergency.

CMS OIS ECloud Support project supports the CMS change requests and defect tracking processes. From tracker in this project, users can make the multiple requests:

1. Delayed defects solving.
   Under track Defects, there are four artifacts that are last modified date are four month ago, but they are still not closed.

See below

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	Artifact ID	Title	Descriptic	Submitted By	Submitted On	Last Modified	Closed	Group	Status	Category	Customer	Priority	Assigned	Reported
2	artf107304	CALT Nexus instability	When	[redacted]	11/20/2012 18:26	1/11/2013 17:06			Open			1	[redacted]	
3	artf107305	Working in Nexus doesn't	It doesn't	[redacted]	11/20/2012 18:31	11/26/2012 17:07			Open			3	[redacted]	
4	artf107306	Sonar SSO doesnt' seem t	I haven't s	[redacted]	11/20/2012 18:33	11/21/2012 10:50			Open			2	[redacted]	
5	artf107307	Use of NTP on TeamForge	This	[redacted]	11/20/2012 18:38	11/21/2012 9:11			Open			2	[redacted]	

2. Delayed implementation of VM Service Requests
   Several artifacts have not been implemented on time: Examples: artf129408 PROD Additional VMs for Tivoli monitoring in PROD environment, CMS approved on May 23, but until June 3, it is still not implemented. artf135242 FFE: add 10G disk to tcffep4r6da10, create a new logical volume and mount /tmp onto it, CMS Approve on May 24, but until June 3, it is still not implemented.

3. Delayed implementation of Infrastructure Change Request
   For example: artf122227 (priority 1) Additional VM Resources for FFE Production VMs. CMS approved on Feb 20, 2013, and assign to implement, but until June 3, it is still not implemented. artf119451 (priority 1): FFE: Change the Network Address Translation (NAT) for the primary interface for server [TCFFE1T1R6WS02]. HHS approved on Feb 11, 2013, and assigns to implement, but until June 3, it is still not implemented.

4. Delay Implementation of CALT Mitigation Issues. These artifacts are almost 2 years of old.

	A	B	C	D	E	F	G	H	I	J	K	L	M
1	Artifact ID	Title	Descriptic	Submittec	Submitted On	Last Modified	Closed	Status	Category	Priority	Assigned	Planned F	Monitorin D
2	artf92797	calt.cms.g	calt.cms.g	[redacted]	8/22/2012 11:19	8/22/2012 11:19		Open	TeamForg	1	[redacted]		
3	artf92794	Memory c	Should be	[redacted]	8/22/2012 11:12	8/22/2012 11:22		Open	TeamForg	1	[redacted]		
4	artf92793	Memory c	Memory c	[redacted]	8/22/2012 11:10	8/22/2012 11:22		Open	TeamForg	1	[redacted]		
5	artf92798	uat.calt.cr	uat.calt.cr	[redacted]	8/22/2012 11:20	8/22/2012 11:20		Open	TeamForg	1	[redacted]		
6	artf92792	Inbound E	CALT relie	[redacted]	8/22/2012 11:09	8/22/2012 11:35		Open	TeamForg	1	[redacted]		
7	artf92804	Schedule	Schedule	[redacted]	8/22/2012 11:37	8/22/2012 11:37		Open		1	[redacted]		
8	artf92818	Firewall c	We need a	[redacted]	8/22/2012 13:54	8/22/2012 13:57		Open	TeamForg	3	[redacted]		
9	artf93068	New DNS	This	[redacted]	8/29/2012 9:39	8/29/2012 11:14		Open	TeamForg	3	[redacted]		

5. Delayed implementation of Report Requests. These artifacts are CMS approved almost a year ago and still did not get implemented.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
1	Artifact ID	Title	Descriptic	Submitter	Submitted On	Last Modified	Closed	Status	Category	Priority	Assigned	Estimated	Remaining	Calculate	Planned F	Required
2	artf7578	Report-4:	Report-4:	[redacted]	2/2/2012 21:58	3/13/2012 11:53		CMS Approved		3	[redacted]	2	2	Not calculated		Report
3	artf47185	Exporting	Sorry for	[redacted]	7/24/2012 20:17	7/24/2012 20:17		CMS Approved		4	None	0	0	Not calculated		

6. Delayed implementation of Service Requests. These artifacts are 3 days delayed

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Artifact	Title	Descrip	Submit	Submitted On	Last Modified	Closed	Status	Catego	Custom	Priority	Assigne	Planne	Comme	Reques
artf135279	Tivoli inst	The	[redacted]	5/24/2013 13:52	5/24/2013 14:58		CMS Approved	Other	OIS	1	[redacted]		Henry wa	[redacted]
artf135239	Tivoli inst	the	[redacted]	5/23/2013 20:31	5/24/2013 15:00		CMS Approved	Other	OIS	2	[redacted]			[redacted]
artf135240	Tivoli inst	The	[redacted]	5/23/2013 21:20	5/24/2013 14:59		CMS Approved	Other	OIS	2	[redacted]		FC	[redacted]
artf135278	Tivoli inst	The	[redacted]	5/24/2013 13:44	5/24/2013 14:56		CMS Approved	Other	OIS	1	[redacted]			[redacted]

Potential Impact: If implementation cannot be finished in a timely manner, then production quality will be impaired.

Recommendation: Once CMS approved change requests, Terremark should implement in the range of SLA.

Source(s):

CALT:
(CMS OIS ECloud Support): Tracker – Defects: artf107304, artf107305, artf107306, artf107307
Tracker – VM Request: artf129408, artf135242
Tracker – Infrastructure Change Request: artf122227, artf119451
Tracker – CALT Mitigation Issues: artf92797, artf92794, artf92793, artf92798, artf92792, artf92804, artf92818, artf93068
Tracker – Report Requests: artf7578, artf47185
Tracker – Service Requests: artf135279, artf135239, artf135240, artf135278

Task: OO-2	Evaluate implementation of the process activities and request volumes to determine if processes are effective and are being followed.	Prob (P)	Impact (I)	Risk Score (P x I)	Risk Level
Finding 3	**Process Deviation:** There are artifacts in CALT (CMS OIS ECloud Support) being updated after they were closed out.	4	2	8	**Moderate**

Finding Detail: In CMS OIS ECloud Support project under tracker - VM Service Request, there 108 closed artifacts, among them 80 are updated after closure. Some are updated even after months of closure. And among these 80 artifacts, 72 are from HIAD project. For example:

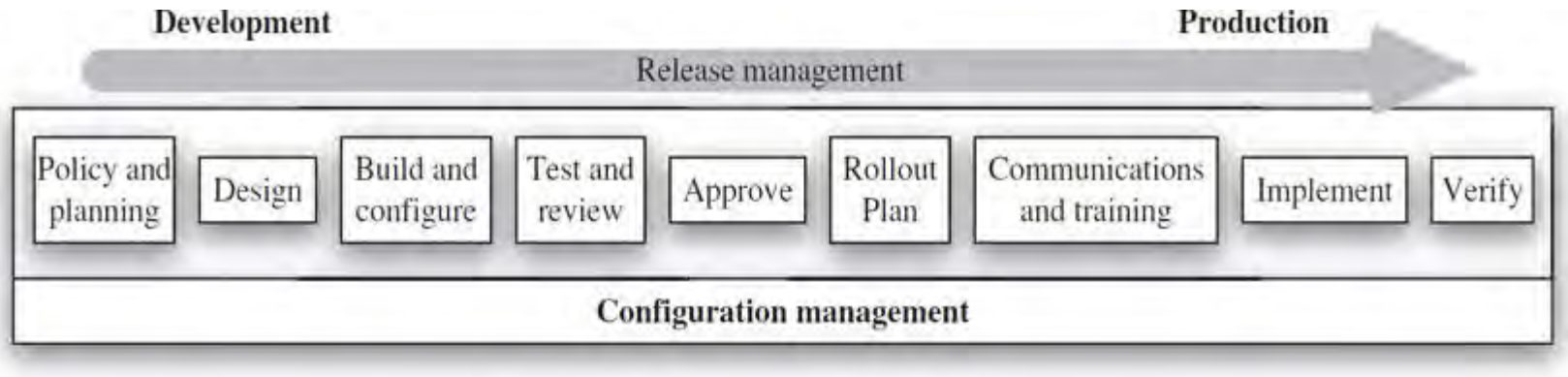
	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	Artifact ID	Title	Descriptic	Submitter	Submitted On	Last Modified	Closed	Status	Category	Customer	Priority	Assigned	Planned F	72 Hour Cu
2	artf107160	FFE: Pleas	FFE: Pleas	[redacted]	11/19/2012 16:10	5/3/2013 8:42	12/18/2012 12:40	Closed	Standard	FFE	2	[redacted]		
3	artf104739	FFE: 2 Nev	FFE: 2	[redacted]	11/5/2012 10:01	5/3/2013 8:42	11/30/2012 11:47	Closed	Standard	FFE	2	[redacted]		
4	artf99726	Connect z	zONE requ	[redacted]	10/17/2012 14:46	5/3/2013 8:42	12/20/2012 13:09	Closed	Standard	DSH	1	[redacted]		
5	artf125948	ECWS VM	VM sprea	[redacted]	3/13/2013 17:08	5/1/2013 15:51	4/1/2013 16:38	Closed	Standard	HIAD	1	[redacted]		
6	artf125623	DSH: PROI	Based on	[redacted]	3/11/2013 16:57	5/1/2013 15:51	3/25/2013 21:07	Closed	Standard	HIAD	3	[redacted]		
7	artf116889	RBIS Test	The RBIS t	[redacted]	1/24/2013 15:14	5/1/2013 15:51	3/22/2013 5:27	Closed	Standard	HIAD	1	[redacted]		
8	artf123454	FFE Test V	Please cre	[redacted]	2/28/2013 6:56	5/1/2013 15:51	3/7/2013 21:13	Closed	Emergenc	HIAD	2	[redacted]		
9	artf124164	add an int	the other	[redacted]	3/4/2013 15:13	5/1/2013 15:51	3/18/2013 17:36	Closed	Standard	HIAD	2	[redacted]		

Potential Impact: Whenever an artifact closes, it should not be updated; otherwise it should be kept open. If customer keeps updated artifact even after it

	closes, it can cause problem of data consistency.				
Recommendation	Update CALT to prevent user to update after close ticket. If they need to do so, they should reopen the ticket and change or create a new ticket.				
Source(s)	**CALT:** artf134754,artf130090,artf130313,artf113972,artf107160,artf104739,artf99726,artf129799,artf126713,artf126730,artf128349,artf130219, artf125948,artf125623,artf116889,artf123454,artf124164,artf123552,artf122790,artf117832,artf119524,artf122263,artf116892,artf118689, artf120131,artf107721,artf117041,artf91500,artf116387,artf115346,artf116732,artf107612,artf112107,artf111948,artf111954,artf107265, artf107877,artf100615,artf107455,artf109267,artf107159,artf105420,artf109192,artf116179,artf100521,artf106314artf103976,artf42432, artf95374,artf99813,artf93146,artf99207,artf103975,artf103980,artf99727,artf97677,artf107452,artf96735,artf105440,artf93022,artf87706, artf87705,artf87704,artf87702,artf87703,artf92780,artf108347,artf108346,artf100497,artf42353,artf42355,artf45234,artf44763,artf115606, artf115604,artf114040,artf42646,artf42354,artf117023,artf126215				
Task: OO-4	**Evaluate impact of system on program goals and performance standards.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Positive Finding:** Benefits are realized through the highly efficient use of the infrastructure and platform tiers to support multiple applications.	N/A			
Finding Detail	A key component of the delivery and architecture model is that benefits are realized through the highly efficient use of the infrastructure and platform tiers to support multiple applications. In contrast to the legacy approach of building an infrastructure to support and manage a single application, the infrastructure supports numerous clouds and the platform supports numerous applications. Cost savings are realized through the sharing of common resources (people, processes and technology) in a secure and efficient manner at each tier. Historically, services needed by an application were built, delivered and utilized by an application-specific provider. The approach often relied on the presumption that to ensure the operability of the application, you must also control the application dependent resources and services. Enterprise Cloud architectures distinctly and deliberately disrupt this paradigm – successfully abstracting platform-level delivery elements from application-specific elements to enable reliable infrastructure and platform services to where diverse applications can be hosted on shared platform and infrastructure components. To achieve the fullest extent of the efficiencies and benefits of this approach, deviation from the shared platform and infrastructure baseline should be minimized, if not precluded in the delivery and support of CCIIO's applications.				
Potential Impact	N/A				
Recommendation	N/A				
Source(s)	**CALT:** doc12895 Enterprise Cloud Roles and Responsibilities Identification and Definition.				
Task: OO-4		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 2	**Verifiability**: Unable to verify if system will perform well under heavy production traffic and impact program goals and performance standards.	3	4	12	**Moderate**
Finding Detail	IV&V team could not verify the system's ability to sustain high traffic due to the lack of evidence of any stress testing performed.				
Potential Impact	If system is not able to perform adequately under heavy production traffic, then this could impact making the provisions of the Affordable				

	Care Act available to the public as expected.				
Recommendation	Perform and capture evidence of volume/stress testing in production system to ensure system will be able to perform as expected when it goes live.				
Source(s)	**GTL:** CLOUD GAP Analysis 20130521 CMS Weekly Status - 4Corner - April 22, 2013 Cloud Computing Services Statement of Work (SOW)				
Task: OO-4		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 3	**Completeness:** Incomplete Service Level Agreement, which might indicate a lack of readiness to go live.	4	3	12	**Moderate**
Finding Detail	doc13116 which contains a tab with a large number of “TBD”s, including the maintenance window data.				
Potential Impact	If a comprehensive SLA plan, Detailed system maintenance plan document is incomplete, then it could impact the vendor’s ability to monitor, track and report on SLA compliance, which is a key delivery in the Cloud Computing Services SOW.				
Recommendation	Complete and publish SLA documentation with all needed information.				
Source(s)	**CALT:** doc13116 SLA Draft Template **GTL:** OptYr2 Mod7 HHS SOW v11				
Task: OO-4		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 4	**Consistency:** There is a difference between the backup requirements and the implemented scheduled backups.	4	3	12	**Moderate**
Finding Detail	The Cloud Computing Services SOW requires daily differential and weekly full backups, while the Asigra implemented backup solution takes what they consider incremental backups each night on only files that have been modified. Is the Weekly full backup required in the SOW assumed to be satisfied with these daily differentials?				
Potential Impact	If full weekly backup is expected and needed for a restore and the functionality is not provided through the daily differentials, then successful restore might be compromised.				
Recommendation	Document if the implemented backup solution satisfies the weekly backup requirement and provide evidence of successful test results.				
Source(s)	**CALT:** doc7475 ECloud Backup Process Document 05_08_2012 **GTL:** OptYr2 Mod7 HHS SOW v11				
Task: OO-4		**Prob**	**Impact**	**Risk Score**	**Risk Level**

		(P)	(I)	(P x I)	
Finding 5	**Process Deviation:** Software license unexpectedly expiring.	4	3	12	**Moderate**
Finding Detail	In production issues meetings there was notification of instances where software license had expired and caused server issues.				
Potential Impact	If software licenses are not monitored and managed correctly, then this could cause production issues and impact program goals and performance standards.				
Recommendation	License management process and documentation should be established and actively managed to prevent lapses in license coverage.				
Source(s)	**Meetings:** Daily CIISG/TM Operations call				
Task: OO-5	**Evaluate operational plans and processes**.	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Correctness:** Release Management revision log doesn't specify the name of the contractor who made the changes to the document.	2	2	4	**Low**
Finding Detail	When reviewing the revision log, It's unclear who made the changes (Apptis, Terremark, Collabnet and CMS). The log shows [redacted] from Apptis, but it's unclear who the other names are ([redacted] .				
Potential Impact	If the revision log doesn't show who made changes, it will be difficult to track the change and hold a specific contractor responsible for that change.				
Recommendation	Revise the revision log and map the names to the contractor to avoid confusion.				
Source(s)	**CALT:** doc12949 PaaS Release Management Plan				
Task: OO-5		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 2	**Consistency:** The revision log has no date for approval for final version, and no CMS approval for V1.2.	2	2	4	**Low**
Finding Detail	Section 4.1 "Assumptions" states that "This Release Management plan is meant to be a living document. Any changes to this plan will be submitted to the COTR for approval". But, there was a change made on 9/10/2012 to V1.2 and the COTR did not approve that change.				
Potential Impact	If CMS doesn't review and sign off on changes to the plan, then it will increase operational risks which can delay operations activities.				
Recommendation	Ensure CMS review date is clearly documented and obtain approval for V1.2.				
Source(s)	**CALT:** doc12949 PaaS Release Management Plan				
Task: OO-5		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 3	**Completeness:** The Release Plan doesn't define a clear release life cycle process.	3	4	12	**Moderate**

Finding Detail	The Release Approach in section 5 states the following: • Release Strategy: The CR will describe how the release will be deployed. • The specific release approach will be determined and recorded for each release. • Release Strategy: Release Content will be included in the CR for the requested approval of the release. • Release Impact: The impact analysis will be a part of the CR governing the release All these approaches mention CR (Change Request) which is part of Change Management. But, there is no indication of Release process including Implementation, Verification, Deployment, Vulnerability Scanning, Penetration Testing, and Configuration Management. The Daily CIISG/TM Operations call that occurs every Monday, Tuesday, Wednesday, and Thursday covers many of the release activities described above, but the process is not documented in the Release Plan.				
Potential Impact	If the Release Management Plan doesn't define a release lifecycle, then there is a risk when new elements are introduced that can disrupt production environment and cause confusion.				
Recommendation	Define the steps for Release Management Process to ensure deployment plans are followed; release packages can be built, installed, tested, and deployed; and knowledge transfer happens with users to optimize use and support of the service. The picture below depicts typical steps of Release Management process.  				
Source(s)	**CALT:** doc12949 PaaS Release Management Plan				
Task: OO-5		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 4	**Correctness**: There is no indication of Release Management process for physical infrastructure (IaaS).	4	3	12	**Moderate**
Finding Detail	It' not clear how a service (VM) will be build, tested, and deployed to meet specifications. The Plan doesn't describe how hardware				

	specification and configuration are pre-defined and tested.
Potential Impact	If there is no Release Management process for physical Infrastructure, then it will be difficult to control the risk when there are numerous scheduled concurrent maintenance activities.
Recommendation	Document Release Management for IaaS including hardware.
Source(s)	**CALT:** doc12949 PaaS Release Management Plan

Task: OO-5		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 5	**Completeness**: The Patch and Vulnerability Management Procedure document Version log is incomplete.	2	2	4	**Low**

Finding Detail

The version log page shows a future date of 9/10/213. Also, there is no evidence that this document was approved by CMS since the approval section is blank.

Date	**Document Version**	**Document Revision Description**	**Document Author**	**Document ID**
10/01/2011	0.1	Document Creation	[redacted]	
9/10/2013	1.0	Annual Review	[redacted]	

Approval Date	**Approved Version**	**Approver Role**	**Approver**	**Document ID**

Potential Impact	If the version control of the document is not accurate, then it will be difficult to find out what changes were made to the document.
Recommendation	Ensure the version control section of the document is correct, and the document is approved by CMS.
Source(s)	**CALT:** doc12886 Patch and Vulnerability Management Procedures.

Task: OO-5		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 6	**Correctness:** There is no separate process for Problem Management.	4	4	16	**High**

Finding Detail	Section 4 of the Incident Management Plan V1.1 describes the Root Cause Analysis (RCA), which appear to be the only documentation related to problem management. Section 3 Approach describes incident Approach not problem approach. **TABLE OF CONTENTS** **1 INTRODUCTION** **2 OVERVIEW** **3 APPROACH** 3.1 INCIDENT IDENTIFICATION AND LOGGING 3.2 INCIDENT CATEGORIZATION AND PRIORITIZATION 3.3 INVESTIGATION AND DIAGNOSIS 3.4 RESOLUTION AND RECOVERY **4 ROOT CAUSE ANALYSIS** **5 GLOSSARY** **6 ACRONYMS**
Potential Impact	If the Problem Management process is not defined separately, then relationships between incidents will not be discovered, and the service may be at risk because no one identified the trends between incidents. Additional resources will be used to solve the same incidents and problems multiple times.
Recommendation	Update section 4 of the Incident Management Plan including trend analysis process, communication process among the teams that must pool their knowledge and expertise to diagnose and resolve the problem, and process for setting up priority levels to ensure there is efficient allocation of resources.
Source(s)	**GTL:** Incident Management Plan V1.1. May 11, 2012

Task: OO-5		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 7	**Correctness:** Event Management process is part of the Incident Management Plan instead of a separate plan.	4	3	12	**Moderate**
Finding Detail	doc12885. OM_Manual_Ecap. Version 1.0, Date: 09.10.12, section 5.3 (Event Management) references the Event Management in the Incident Management. These two activities are not the same and should be documented separately. Event Management monitors all Events to ensure normal operation. It handles normal messages as well as detects, escalates and reacts to exceptions. Incident Management on the other hand concentrates on restoring unexpectedly degraded or disrupted services to users as quickly as possible, in order to minimize business impact.				

Potential Impact	If Event Management process is mixed with Incident Management, then it would be difficult to distinguish between the two processes. There will be a risk to operation if an incident is classified as an Event by mistake.				
Recommendation	Ensure Event Management Process is document separately and clarify the different types of events including: • Informational: such as notification of a scheduled job finishing or a user accessing an application. • Warning: including indications that utilization of a particular CI has reached a certain threshold, such as 75 per cent, of capacity. • Exception: such as unauthorized software detected or a capacity threshold has been breached.				
Source(s)	**CALT:** doc12885 OM Manual eCAP				
Task: OO-6	**Evaluate implementation of the process activities including backup, disaster recovery and day-to-day operations to verify the processes are being followed.**	**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 1	**Process Deviation**: The Release Management process is not being followed	5	4	20	**High**
Finding Detail	The daily CIISG/TM Ops meeting covers Cloud operations issues, but the meeting doesn't seem to be planned and organized. Contractors are asking for the status on VM configuration, change requests updates, Outages, and patches, and Cloud Vendor is making decisions on the spot. Decisions are made verbally only to the people who are in attendance, and not documented anywhere.				
Potential Impact	If Release Management process is not being followed, then coordination and communication will be difficult and the CMS wider audience will not get the message on time to adjust their progress. .				
Recommendation	Ensure implementation of the process is thoroughly addressed. Document Release Process Activities during CIISG/TM meetings and ensure that decisions are posted in CALT for all stakeholders to review.				
Source(s)	**CALT:** doc12949 PaaS Release Management Plan **Meetings**: Daily CIISG/TM Ops 05152013				
Task: OO-6		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 2	**Completeness:** No Configuration Management Database (CMDB).	3	4	12	**Moderate**
Finding Detail	The SOW states that Terremark will provide information that can be used in Root Cause Analysis for potential issues. The lack of the standard ITIL configuration management database will slow down the analysis of root causes of problems				
Potential Impact	If there is no CMDB, then the analyses of root causes will take longer and could impact the development of solutions to problems causing delay in plans.				
Recommendation	Implement a Configuration Management Database				
Source(s)	**GTL:** OptYr2 Mod7 HHS SOW v11.doc **Interview:** Cloud Computing Assessment Discussion with Terremark 05232013				

Task: OO-6		Prob (P)	Impact (I)	Risk Score (P x I)	Risk Level
Finding 3	**Consistency:** Problem management is not implemented separately from incident management in CALT.	4	4	16	**High**
Finding Detail	Artf134788. This ticket was submitted on 5/20/13 as high priority by submitter and business, status: pending. The description of the incident is: FFE: EMERGENCY--- MANY servers in read-only state after this weekend's event. Need URS to check ALL file systems ASAP. However, during the status meetings calls the following week, and the weekly CMS Project Management Office (PMO) there was no attempt to look into this problem in more details and conduct a RCA.				

Artifact I	Title	Descriptio	Submitted By	Submitted Or	Last Modifiec	Status	Catego	Custo	Pric	Assigne	Planne	Begin Date	Begin T	Busine	Inciden	Root Ca
artf122653	HIOS Web	[redacted]		2/20/2013 13:49	3/5/2013 17:04	In Progress			2	[redacted]		2/20/2013 0:00		High	Multiple Customer	
artf133121	FFE: 10.15	due to an u	[redacted]	5/6/2013 11:47	5/21/2013 19:50	Pending C	Other	FFE	1	[redacted]				High	Single Cus	Initial
artf133202	HIOS: Can	[redacted]		5/7/2013 13:51	5/7/2013 17:43	Pending		HIOS	1	[redacted]		5/7/2013 0:00		High	Multiple Customer	
artf134788	FFE: EMER	FFE: EMERGENCY	[redacted]	5/20/2013 10:05	5/21/2013 14:56	Pending C	PaaS	FFE	[redacted]					High		
artf134798	TWS not a	Connection	[redacted]	5/20/2013 10:59	5/22/2013 10:48	Pending C	Applicatic	DSH	1	[redacted]		5/20/2013 0:00		High		

Potential Impact	If problems are not tracked separated from Incidents, then the cloud team won't be able to link similar incidents to find out what the problem is. No RCA will be performed and the service may be at risk.				
Recommendation	Ensure that a single tracking process that interfaces with the incident management process is in place to assist in providing the audit trail and status required to monitor problems. In addition, ensure continuous communication with the impacted parties at all stages so that they can get the appropriate solution in a timely fashion.				
Source(s)	**GTL:** Incident Management Plan V1.1. May 11, 2012.				
Task: OO-6		**Prob (P)**	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 4	**Consistency**: IaaS problems (root cause of an incident) are not tracked consistently.	5	5	25	**High**
Finding Detail	During the daily CIISG/TM Operations call on 5/22/13, URS stated that the CMS Weekly Status/ 4 Corner Report May 20, 2013 shows a huge spike in Bandwidth. CMS GTL was surprised and no further action was taken during that meeting or the next day meeting. A noticeable spike in Bandwidth is a major problem and Terremark (TM) should have recommended a root cause analysis of this incident. Also, the Agenda of the Exchange IT PMO Meeting, May 22, 2013, page3 stated "Over the weekend (5/18, 5/19) there was a hardware failure at the TM data center which affected most of DSH environments including PROD and prolonged the PM deployment. The failed hardware was replaced by TM on 05/19 at 7 AM; Team validated all the DSH environments, addressing connectivity issues and performed a				

	smoke test". The IV&V team can't find evidence that root cause analysis was conducted and documented in CALT about this problem.
Potential Impact	If root cause analysis is not performed as quickly as possible when problems occur, then it will be difficult to prevent or minimize the impact of the problem.
Recommendation	Ensure that the root cause analysis is performed and documented in CALT. Ensure result of the analysis is communicated to all stakeholders and can be used as lessons learned.
Source(s)	**GTL:** CMS Weekly Status/ 4 Corners Report May 20, 2013 Incident Management Plan, V1,1, May 11, 2012 **Meetings**: Daily CIISG/TM Operations call. 5/22/13 Exchange IT PMO Meeting MOM: May 22, 2013- Agenda **Interview**: Cloud Computing Assessment Discussion with Terremark 05232013

APPENDICES

APPENDIX A: ACRONYMS

Acronyms used in this document are listed below.

Acronym	Description
ACA	Patient Protection and Affordable Care Act
ALM	Application Lifecycle Management
ATO	Authority to Operate
CALT	Collaborative Application Lifecycle Tool
CCB	Change Control Board
CCIIO	Center for Consumer Information and Insurance Oversight
CIISG	Consumer Information & Insurance Systems Group
CLIN	Contract Line Item Number
CMMI	Capability Maturity Model Integration
CM	Configuration Management
CMDB	Configuration Management Database
CMP	Change Management Plan
CMS	Centers for Medicare & Medicaid Services
COTR	Contracting Officer's Technical Representative
COTS	Commercial-Off-The-Shelf
CR	Change Request
C&A	Certification and Accreditation
DSH	Data Services Hub
eCAP	CCIIO Cloud Application Platform
FEDRAMP	Federal Risk and Authorization Management Program
FEPS	Federal Exchange Program System
FFE	Federally Facilitated Exchange
FFP	Firm Fixed Price
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
FMPS	Federal Marketplace Program System
GSS	General Support System
GTL	Government Task Lead
GUI	Graphical User Interface
HIAD	Health Insurance Assistance Database
IaaS	Infrastructure as a Service
IEEE	Institute of Electrical and Electronics Engineers
IMS	Integrated Master Schedule
IT	Information Technology
ITIL	Information Technology Infrastructure Library
IV&V	Independent Verification and Validation
MIDAS	Multidimensional Insurance Data Analytics System
N/A	Not Applicable
NAP	Network Access Protection
NAT	Network Address Translation
NIST	National Institute of Standards and Technology
OE	Operating Environment
OIS	Office of Information Systems
OM	Operations and Maintenance
OO	Operations Oversight

Acronym	Description
PaaS	Platform as a Service
PDA	Personal Data Assistant
PISP	Policy for the Information System Program
PMO	Project Management Office
PMBOK	Project Management Institute's Project Management Body of Knowledge
POAM	Plan of Action and Milestone
QHP	Quality Health Plan
QSSI	Quality Software Services, Inc.
RM	Requirements Management
RMP	Risk Management Plan
RCA	Root Cause Analysis
SEI	Software Engineering Institute
SLA	Service Level Agreement
SOW	Statement of Work
SSP	System Security Plan
ST	System Testing
TBD	To Be Determined
TM	Terremark
TRA	Technical Reference Architecture
URS	United Research Services
VM	Virtual Machine
V&V	Verification and Validation
XLC	Expedited Life Cycle

APPENDIX B: STAKEHOLDER INTERVIEW/MEETING

Table B-1 Interviews and Meetings

Name	Interview	Date
[redacted]	Cloud Computing Assessment Discussion with Terremark	4/30/2013
[redacted]	IV&V CALT Demo Interview	5/13/2013
[redacted]	Cloud Computing Assessment Discussion with Terremark	5/21/2013
[redacted]	Cloud Computing Assessment Discussion with Terremark	5/23/2013
	Meeting	
	CCB IT Operational Meeting	5/21/2013
	Exchange IT PMO Meeting	5/22/2013
	MIDAS Daily Scrum	Daily
	CIISG/TM Ops meeting	Daily
	Daily Morning Production Call	Daily

APPENDIX C: REVIEWED DOCUMENTATION

Table C-1 Reviewed Documentation

Document Element #	Document ID #	Document/Information Received	Source
D01	doc12863	PaaS_SOP_Personnel Security Mgmt_09062012	CALT
D02		OptYr2 Mod7 HHS SOW v11	GTL
D03	doc12859	CFACTS CSP4 PaaS System Security Plan Final090412	CALT
D04	doc12381	FFE_HTD	CALT
D05	doc17091	MIDAS SSP	CALT
D06	doc17090	MIDAS ISRA	CALT
D07		20130426 Welcome Guide to Enterprise Cloud Federal Version LAN	GTL
D08		Center-for-Consumer-Information-and-Insurance-Oversight-TMRK_CSP4IaaS-ATO Memo 2013	GTL
D09	doc12879	TMRK PaaS GSS FIPS-199 SYSTEM SECURITY LEVEL	CALT
D10		CMS Weekly Status - 4Corner - April 22, 2013	GTL
D11	doc12881	Backup and Restore Services procedures	CALT
D12	doc7475	ECloud Backup Process Document 05_08_2012	CALT
D13	doc12885	OM Manual eCAP	CALT
D14	doc12880	VM Software Components	CALT
D15	doc12865	CCIIO VLAN design v2.6	CALT
D16	doc20174	MIDAS_Operations and Maintenance Manual	CALT
D17	doc6568	CMS eCloud Contingency Plan 093011 v7	CALT
D18	doc19387	DE-1 DE-2 MIDAS Private Cloud Impl Env Server Specifications v2.0	CALT
D19	doc19388	MIDAS Private Cloud Test Env Server Specifications v2.0	CALT
D20	doc19391	OE-5 OE-7 MIDAS Software Tools List	CALT
D21	doc12925	DSH_ARC_Overview_v2	CALT
D22		Services	GTL
D23		CCIIO Resource Allocations by Project - ECPE Cloud 20130419 SOW	GTL
D24	doc13247	Capacity Planning 10-17-12	CALT
D25	doc11023	CSP4IaaSArtifactsUpdate091212 (folder)	CALT
D26		OptYr2 Mod 7 HHS SOW (CMS Cloud)v11	GTL
D28	doc12949	PaaS Release Management Plan	CALT
D29	doc8175	Cloud_Processes	CALT
D30		CMS Weekly Status - 4Corner - May 20, 2013 -REV A	GTL
D31		CCMS TRA Virtualization Supp v 1 1_07282010	GTL
D32	doc12975	CMS eCloud Governance – Contingency Plan	CALT
D33	doc10998	PaaS C&A Artifacts 2	CALT
D34	doc6148	MIDAS Server Specifications v0.7	CALT
D35	doc8179	Provisioning Process Legend	CALT

D36		IVV Questionnaire_Terremark Responses May 20 2013	GTL
D37		CLOUD GAP Analysis 20130521	GTL
D38		CCIIO Enterprise Cloud Infrastructure 3-Zone Architecture with Defined Regions	GTL
D39	doc10229	SCA and Cloud GSS 08102012-2	CALT
D40	doc30440	Configuration_Management_Plan_v1.2 09062012	CALT
D41	doc12461	PM_R3S9_EHB_OpsMaintManual	CALT
D42	doc2475	Exchange Reference Architecture Foundation Guide	CALT
D43	doc2744	CMS TRA Web Services Suppl_Draft V06_052311	CALT
D44	doc12878	TMRK CSP4PaaS RA Final 09062012	CALT
D45	doc12864	CCIIO PaaSCloud VLAN Assignments (1)	CALT
D46	doc12865	CCIIO VLAN design v2.6, doc12866-CCIIO VLAN Shared Services v2.5	GTL
D47	doc12851	CALT CFACTS CM Plan	CALT
D48	doc13102	Platform delivery process	CALT
D49	doc28366	IaaS FY2013 Attestation Input	CALT
D50		CMS Federal Enterprise Architecture (FEA), CMS Technical Reference Architecture (TRA)	Standards
D51		CMS Technical Reference Architecture – Private and Community Cloud IaaS and PaaS Infrastructure Supplement.	Standards
D52	doc13090	Provisioning Process Legend	CALT
D53	doc8177	Platform Delivery Process v02	CALT
D54	doc11232	FFE_ArchitecturalDiagrams_Internal	CALT
D55	doc12461	PM_R3S9_EHB_OpsMaintManua	CALT
D56	doc5749	MIDAS System Design Document	CALT
D57	doc26320	DSH_IMP_OMM	CALT
D58	doc26316	DSH_PLAN_CONOP	CALT
D59	doc12886	Patch and Vulnerability Management Procedure	CALT
D60	doc12950	PaaS Change Management Plan	CALT
D61	doc12873	Enterprise Cloud Roles and Responsibilities Identification and Definition v 1 0	CALT
D62	doc12862	Incident Management Plan_v.7.docx	CALT
D63	doc12895	Enterprise Cloud Roles and Responsibilities Identification and Definition	CALT
D64	doc13116	SLA Draft Template	CALT
D65		Incident Management Plan V1.1. May 11, 2012	GTL

APPENDIX D: RISK DETERMINATION

D.1 RISK DESCRIPTION

Findings identified in this assessment must be associated with several metrics factors to help determine the level of risk value related to a specific element or process. Risk is defined as the combination of the probability of occurrence and the consequences of a given future undesirable event. Risk can be associated with products and/or projects.

The determination of risk or vulnerability can be expressed as a function of:

- The likelihood (probability) of a given finding posing a risk to system development or functionality
- The magnitude of the impact of a finding posing a risk to system development or functionality

Where:

P = Probability
I = Impact
and: P x I = Risk Score

To measure risk, a risk scale and a risk-level matrix has been developed.

D.2 RISK DETERMINATION

Table D-1 displays the Risk Scale and required actions. This risk scale, with its ratings of High, Moderate, and Low, represents the degree or level of risk to which a system, facility, or procedure might be exposed to a given vulnerability were exercised. The risk scale also presents actions that senior management, the mission owners, must take for each risk level.

Table D-1 Risk Scale and Necessary Actions

Risk Rating	Action Implementation
High	High-risk levels create a strong need for corrective actions and the creation of an action plan that is put in place as quickly as possible.

Risk Rating	Action Implementation
Moderate	Moderate-risk levels warrant corrective actions and a plan to incorporate those actions within a reasonable period of time.
Low	For low-risk levels, the application owner must decide whether corrective actions are needed or whether the risks may be accepted.

D.3 RISK MITIGATION AND RECOMMENDATIONS

During the risk mitigation process, controls that could mitigate or eliminate the identified risks are provided. The goal of the recommended controls is to reduce the level of risk to FMPS and its data to an acceptable level. The following factors should be considered in recommending controls and alternative solutions to minimize or eliminate identified risks:

- Effectiveness of recommended options (e.g., system compatibility)
- Organizational policy
- Operational impact

For consistency and clarity and to maintain an accurate understanding of risk findings, IV&V adopted the CMS risk management methodology, as defined in the Risk Management Plan (CMS RMP – '*CMS Health Insurance Exchange Risk Management Plan v 1.1_04302012_Draft'*); accordingly, risks identified on the FFE project level will be shared with partner and stakeholder groups for visibility and shared understanding of FMPS project risks to support successful risk management at the project level and through the enterprise level through correlation to the FFE Integrated Master Schedule (IMS) milestones and tasks. The intent is to identify and appropriately address and elevate project risks to the Health Insurance Exchange Program level for visibility, mitigation and for possible action.

Each risk is documented as fully as possible to include probability (likelihood), impact, risk value, system & scope assessment area and overall characteristic. As a part of the documentation of the risk, a nominal probability (likelihood) and impact rating on the risk finding was submitted and was mathematically factored to reach an overall risk value. See Tables 2-3, 2-4, and 2-5 for probability, impact and risk value guidance.

Table D-2 Probability Assessment Criteria

Level	Probability	Probability of Occurrence
5	Near Certainty	81-99%
4	Highly Likely	61-80%
3	Likely	41-60%

Level	Probability	Probability of Occurrence
2	Low	21-40%
1	Not Likely	5-20%

Table D-3 Impact Assessment Criteria

Level	Impact
5	Severe degradation in technical threshold performance; jeopardizes project success. Cannot meet key milestones. Represented as a 20% deviation of the baselined plan.
4	Significant degradation in tech performance, unacceptably below goals, no design margins. Requires program or project critical path change. Represented as a 15–20% deviation of the baselined plan.
3	Moderate shortfall in tech performance, with limited impact; technical goals unmet and design margins significantly reduced. Schedule slip impacts milestone (MS) or Critical path slack. Represented as a 10–15% deviation of the baselined plan.
2	Minor reduction in technical performance, but can be tolerated, little impact; goals and design margins reduced. Schedule slip but will meet MS. Represented as a 5–10% deviation of the baselined plan.
1	Minimal consequence to performance, but no overall impact; goals and design margins will be met. No schedule slip. < 1% increase from baseline.

Table D-4 Risk Value

Risk Value Exposure Score	Risk Level
15-25	High
6-14	Moderate
1-5	Low

Exhibit 14

TurningPoint. Federal Marketplace Program System (FMPS) Independent Verification & Validation (IV&V) Assessment 9 Report. July 11, 2013.

CENTERS FOR MEDICARE & MEDICAID SERVICES

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

Federal Exchange Program System (FMPS)

Independent Verification & Validation (IV&V) Assessment 9 Report (Readiness Review Template)

Version 1.0

July 11, 2013

Prepared by:

TurningPoint
TurningPoint Global Solutions
Software Services Company™

Document Number: FMPSIV&V-IAR-09-TP
Contract Number: HHSM-500-2012-00008U

CMS SENSITIVE INFORMATION—REQUIRES SPECIAL HANDLING

APPROVALS

Exchange IT Program Approving Authority:

Signature	Printed Name	Date	Phone Number

Monique Outerbridge, CMS/OIS/CIISG, Director

Signature	Printed Name	Date	Phone Number

[redacted], CMS/OIS/CIISG

Signature	Printed Name	Date	Phone Number

[redacted] CMS/OIS/CIISG, Government Task Lead

REVISION HISTORY

Version	Date	Organization/Point of Contact	Description of Change
1.0	07/11/2013	TurningPoint	Initial submission

Table of Contents

EXECUTIVE SUMMARY **1**

1 INTRODUCTION **2**

1.1 BACKGROUND 2
1.2 SCOPE 2
1.3 FMPS OVERVIEW 2
1.4 IV&V APPROACH AND METHODS 2
1.5 ASSUMPTIONS 4
1.6 CONSTRAINTS 4
1.7 REFERENCES 4

2 FMPS READINESS REVIEW TEMPLATE **5**

APPENDICES **9**

APPENDIX A: ACRONYMS **10**

APPENDIX B: STAKEHOLDERS INTERVIEWED **11**

APPENDIX C: DOCUMENTATION REVIEWED **12**

APPENDIX D: RISK DETERMINATION **13**

D.1 RISK DESCRIPTION 13
D.2 RISK DETERMINATION 13
D.3 RISK MITIGATION AND RECOMMENDATIONS 14

Figures

Figure 1: Total Findings by Risk Level 1

Tables

Table 1: Findings by Area 1
Table 1.4-1: Findings Table Terminology 3
Table 1.4-2: Findings Categories 3
Table B-1 Interviews & Meetings 11
Table C-1 Documentation Reviewed 12
Table D-1 Risk Scale and Necessary Actions 13
Table D-2 Probability Assessment Criteria 14
Table D-3 Impact Assessment Criteria 15
Table D-4 Risk Value 15

EXECUTIVE SUMMARY

This report presents the results of a short assessment of the Readiness Review Template by the Independent Verification & Validation (IV&V) contractor, TurningPoint Global Solutions, which was tasked by the Centers for Medicare and Medicaid Services (CMS) to provide monthly technical audits of the Federal Marketplace Program System (FMPS).

Table 1 below depicts the total findings by area broken out by risk level.

Table 1: Findings by Area

Total Findings				
	Low	Moderate	High	Total
FMPS Readiness Review Template	4	3	1	8

Figure 1 displays a summary of total findings by risk level.

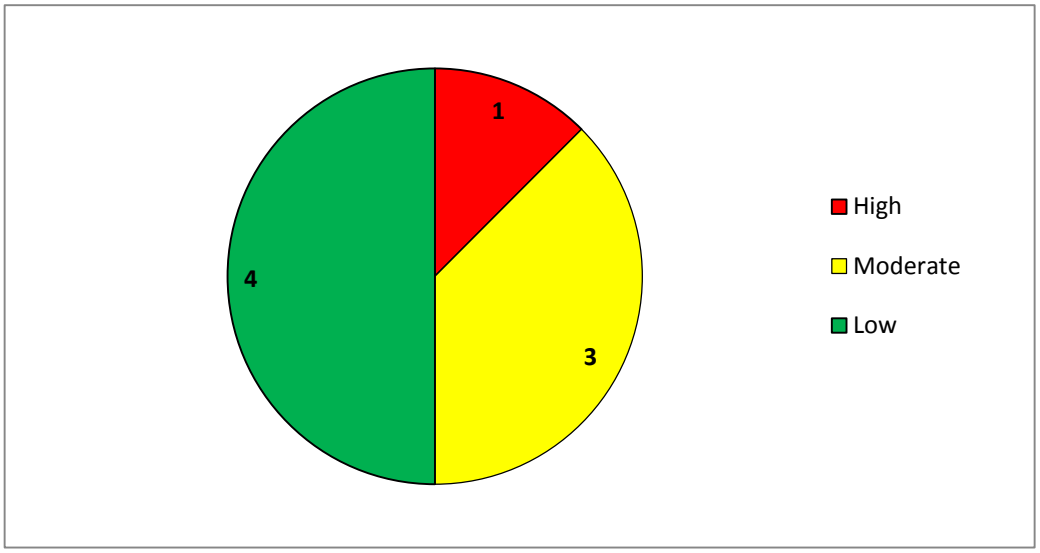


Figure 1: Total Findings by Risk Level

Recommendation:

- Determine the minimum essential components that must be in place for October 1, 2013, and make these high priority items.
- Determine what kinds of defects must absolutely be fixed before October 1, 2013 and which ones can be delayed.

1 INTRODUCTION

1.1 BACKGROUND

The FMPS program was initiated by CMS to provide health insurance exchange capabilities required by the Patient Protection and Affordable Care Act (ACA) of 2010. In support of the FMPS effort, CMS employed TurningPoint to provide an independent and unbiased analysis of the FMPS components and artifacts. CMS tailored the IEEE 1012 standard to 106 V&V service areas covering the nine Scope of Service areas in the FMPS IV&V Statement of Work (SOW): Quality Management, Training, Requirements Management, Operating Environment, System and Acceptance Testing, Data Management, and Operations Oversight. Not all service areas will be covered in all assessments.

1.2 SCOPE

The scope of this assessment is the FMPS Readiness Review Template.

1.3 FMPS OVERVIEW

The IV&V team analyzed and organized the assessment of the FMPS Readiness Review Template under the following service area:

- Operations Oversight

1.4 IV&V APPROACH AND METHODS

For this assessment, the FMPS IV&V Team's approach included: planning the scope of the assessment and identifying the standards to use. The IV&V approach to working with federal and contractor organizations is cordial and supportive of priorities, while maintaining independence and objectivity during the assessment.

The findings are only related to the Readiness Review Template. Each finding includes an IEEE categorization, impact statement, sources, risk probability, risk impact, and risk value. See Appendix D: Risk Determination for more detailed information about the method used to determine risk impact, probability and value.

Table 1.4-1 below defines the terminology used in findings tables.

Table 1.4-1: Findings Table Terminology

Findings Table Heading	Description
Task Number	Pulled from FMPS IV&V SOW
Task Description	Pulled from FMPS IV&V SOW
Finding	Based on category description table below
Finding Description & Evidence	Results of IV&V evaluation
Source	List of information source used to make determinations
Recommendation	Results of IV&V evaluation

A Finding or Anomaly is anything observed in the documentation or operation of software that deviates from expectations based on previously verified software products or reference documents (IEEE 1012).

Table 1.4-2 below depicts the definition of finding categories used in the tables in this report.

Table 1.4-2: Findings Categories

Category	Description
Future Assessment	This area was not assessed by IV&V during this reporting period.
No "X" Activity Occurred	No project activity occurred in the area of "X" for the scope of this assessment.
Process Deviation	Documentation or practices indicate the project has deviated from the defined and approved policy, process or procedure.
Completeness	The state of being complete and entire; having all necessary parts, elements, or steps.
Correctness	(1) The degree to which a system or component is free from faults in its specification, design, and implementation. (2) The degree to which software, documentation, or other items meet specified requirements. (3) The degree to which software, documentation, or other items meet user needs and expectations, whether specified or not (Wikipedia).
Consistency	The degree of uniformity, standardization, and freedom from contradiction among the documents or parts of a system or component (IEEE 1012).
Accuracy	(1) A qualitative assessment of correctness, or freedom from error. (2) A quantitative measure of the magnitude of error. (IEEE 610.12-1990)
Readability	Readability is the ease in which text can be read and understood by people. The readability of a program is related to its maintainability, and is thus a critical factor in overall software quality.
Positive Finding	This area was assessed by IV&V and the following positive items are noted.
Verifiability	(1) The extent to which the evaluation of a system or component can be performed. (2) The extent to which the correctness of a system can be determined
Testability	(1) The degree to which a system or component facilitates the establishment of test criteria and the performance of tests to determine whether those criteria have been met. (2) The degree to which a requirement is stated in terms that permit establishment of test criteria and performance of tests to determine whether those criteria have been met (IEEE 610.12-1990).

Category	Description
Traceability	The ability to link product requirements back to stakeholders' rationales and forward to corresponding design artifacts, code, and test cases. Traceability supports numerous software engineering activities such as change impact analysis, compliance verification or trace back of code, regression test selection, and requirements validation. It is usually accomplished in the form of a matrix created for the verification and validation of the project.
No change	This area was assessed by IV&V and no change was found between this assessment and the previous one.
Process Improvements	This is an area that has no problems in correctness, completeness, consistency or accuracy. It is only an area identified for possible improvement.

1.5 ASSUMPTIONS

The FMPS IV&V team made the following assumptions during this assessment:

- The files delivered to the FMPS IV&V Team by email are the only Readiness Review Templates used for review.

1.6 CONSTRAINTS

The IV&V team was constrained by the following during this assessment:

- This was a quick review where the files were received on July3, 2013 and a turnaround was provided on Tuesday, July 9, 2013.

1.7 REFERENCES

The standards listed below were utilized for the IV&V team's review of the IMS files and in the preparation of this report.

- IEEE Standard for Software Verification and Validation 1012-2004
- The *PMBOK® Guide*—Fourth and Fifth Editions

2 FMPS READINESS REVIEW TEMPLATE

This section covers detailed findings of the review of the Readiness Review template.

IV&V Task: OO-6	Evaluate implementation of the process activities including backup, disaster recovery and day-to-day operations to verify the processes are being followed.	Prob (P)	Impact (I)	Risk Score (P x I)	Risk Level
Finding 1	**Completeness:** There is no overarching framework with which to aggregate the status information and ensure the information is complete during the Readiness Review. The use of the template to collect and present information by contractor fails to provide the high-level or business-wide view.	5	4	20	**High**
Finding Detail	It has been stated on more than one occasion that meeting participants have a lack of understanding of project-wide information, and therefore, some people are surprised at the tasks that still need to be performed. This high-level understanding should not just reside within a few of the FMPS architects and senior managers. It should be shared, and the status should be communicated to all of the stakeholders on a regular basis. This could be best presented in an overarching framework when information is gathered and presented.				
Potential Impact	If information is not aggregated to provide an enterprise view of completeness, then some areas of work may not be performed on time or at all. This will impact budget and schedule.				
Recommendation	• Update the Blueprint (or equivalent) and use it as an aggregation tool to ensure all business processes are covered. • Collect the information by contractor, but aggregate it by business process using the Blueprint (or equivalent) for presentation in the Readiness Review.				
Source(s)	**Direct:** Health Insurance Marketplace June IT Readiness Review, v. 2, July 2, 2013 **Meeting:** June Marketplace Readiness Review – 6/27/13				
		Prob (P)	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 2	**Correctness:** The Program presents status information almost completely from an IT-centric perspective. A business customer-oriented high-level perspective should be used in Readiness Reviews.	4	3	12	**Moderate**
Finding Detail	The FMPS Program shares information from an IT-centric perspective among the IT stakeholders. This fails to provide IT stakeholders with the visibility into the business and customer priorities. Slide 4 mentions “business operations.” Slide 5 shows only 5 components of business operations. On Slide 8, there is a section for Business Operations, with areas of business support for IT. However, IT should be supporting the business, not the reverse.				
Potential Impact	If the business perspective and status are not being shared on a regular basis, then individual IT stakeholders may fail to establish correct priorities, and it may be too late before they are discovered requiring adjustments in scope, or causing schedule delays and increased costs. This is even more important as the deadlines approach.				

Recommendation	• Present information from a customer-oriented perspective. • Ensure that the impact of risks and workarounds are stated from a customer-oriented perspective. • Include the business, not an IT person that serves as the business liaison, in the Readiness Review.				
Source(s)	**Direct** Health Insurance Marketplace June IT Readiness Review, v. 2, July 2, 2013 **Meeting:** June Marketplace Readiness Review – 6/27/13				
		Prob (P)	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 3	**Correctness:** Most of the graphical representations are too busy to provide stakeholders with a clearer understanding of the Program's milestones and they do not meet Section 508 requirements.	4	1	4	**Low**
Finding Detail	Usually graphics are used to present information visually when words are less able to do so. It is difficult to understand the graphics presented on Slide 6. There are also a lot of colors that are presented without shading; this does not meet Section 508 requirements.				
Potential Impact	If too many items and too much color are used in graphics, then communication of the information may be impeded.				
Recommendation	• Use colors and shading to emphasize areas of importance (tasks are late, this is high risk, task needs management attention). • Provide a "Zoomed out" view where details make the graphics too busy. Use backup text to provide the details. • Follow Section 508 guidelines when presenting information.				
Source(s)	**Direct** Health Insurance Marketplace June IT Readiness Review, v. 2, July 2, 2013				
		Prob (P)	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 4	**Completeness:** The topics of training, user documentation and knowledge transfer appear to be missing from the Standard Readiness Outline on Slide 8.	2	2	4	**Low**
Finding Detail	These items may be embedded in the detail of the other tasks; on some of the slides they seem to be present. However, these are normally tasks that are addressed at a higher level in a readiness assessment.				
Potential Impact	If these tasks are not included in the readiness review, then issues relating to the tasks may not be uncovered in time for early management action.				
Recommendation	• Include the topics of training, user documentation and knowledge transfer in the outline.				
Source(s)	**Direct** Health Insurance Marketplace June IT Readiness Review, v. 2, July 2, 2013				
		Prob (P)	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**

Finding 5	**Process Improvement:** Suggest that a high level slide of development status and risk be used to determine if a deep-dive on details is needed during the review.	2	2	4	**Low**
Finding Detail	There are a lot of slides and a lot of detail required for the readiness review. Instead, a high level slide could be presented, using color to provide development status (on target, at risk, etc.). For areas of risk and issues, more detail could be provided for a deep dive by management. Also, development status is needed first to determine the content of a release. So, the order could perhaps be improved by presenting development status before covering release content decisions.				
Potential Impact	If too many slides are used to present status, then management will not be able to cover all of the slides (as in the 6/127/13), and important areas may not be addressed.				
Recommendation	• Cover an overview slide on development status prior to the release slide. • For on-target areas, keep detailed slides as backup.				
Source(s)	**Direct** Health Insurance Marketplace June IT Readiness Review, v. 2, July 2, 2013				
		Prob (P)	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 6	**Process Improvement:** Ensure that all risks include the recommendation for mitigation and issues include a recommendation for action.	2	2	4	**Low**
Finding Detail	The risks and issues sections do not include the organizations recommendations for mitigation and action. The organization closest to the risk or issue may have the best knowledge about actions that should be performed next.				
Potential Impact	If the organization that identified a risk or issue with a component does not provide a recommendation for mitigation or action, then the most optimal actions may not be taken.				
Recommendation	• Add space and require recommendations for identified risks and issues.				
Source(s)	**Direct** Health Insurance Marketplace June IT Readiness Review, v. 2, July 2, 2013				
		Prob (P)	**Impact (I)**	**Risk Score (P x I)**	**Risk Level**
Finding 7	**Accuracy:** There is no independent verification of reported readiness status or risks during readiness reviews, so the information may be inaccurate.	3	3	9	**Moderate**
Finding Detail	The readiness statuses being reported by the various contractors do not include evidence of independent verification.				
Potential Impact	If there is no independent verification of readiness status, then the statuses could be inaccurate.				
Recommendation	• Consider adding independent verification as a part of readiness reviews. • Consider adding the independent documentation of risks.				
Source(s)	**Direct** Health Insurance Marketplace June IT Readiness Review, v. 2, July 2, 2013				

		Prob (P)	Impact (I)	Risk Score (P x I)	Risk Level
Finding 8	**Completeness:** Priorities do not seem to be a part of readiness reviews to ensure that the most critical functionality is in place by Oct. 1.	4	2	8	**Moderate**
Finding Detail	The use of priorities appears to be missing from the readiness template. These would ensure that the most critical functionality is in place on Oct. 1 or earlier.				
Potential Impact	If all functionality is treated with the same priority, then if trade-offs have to be made during readiness reviews, the information will not be available and management attention may not be focused on the higher areas of risk.				
Recommendation	• Prioritize critical functionality.				
Source(s)	**Direct** Health Insurance Marketplace June IT Readiness Review, v. 2, July 2, 2013				

APPENDICES

APPENDIX A: ACRONYMS

Acronyms used in this document are listed below.

Acronym	Description
ACA	Patient Protection and Affordable Care Act
CALT	Collaborative Application Lifecycle Tool
CIISG	Consumer Information & Insurance Systems Group
CMS	Centers for Medicare & Medicaid Services
FMPS	Federal Marketplace Program System
FFM	Federally Facilitated Marketplace
IEEE	Institute of Electrical and Electronics Engineers
IT	Information Technology
ITIL	Information Technology Infrastructure Library
IV&V	Independent Verification and Validation
N/A	Not Applicable
OO	Operations Oversight
PMBOK	Project Management Institute's Project Management Body of Knowledge
RMP	Risk Management Plan
SOW	Statement of Work
V&V	Verification and Validation

APPENDIX B: STAKEHOLDERS INTERVIEWED

Table B-1 Interviews & Meetings

There were no interviews or meetings for this assessment. It is limited to documentation only.

APPENDIX C: DOCUMENTATION REVIEWED

Table C-1 Documentation Reviewed

Document Element #	Document ID #	Document/Information Received	Source
D01	N/A	Health Insurance Marketplace June IT Readiness Review, v. 2, July 2, 2013	Direct
D02	N/A	June Marketplace Readiness Review – 6/27/13	Meeting

APPENDIX D: RISK DETERMINATION

D.1 RISK DESCRIPTION

Findings identified in this assessment must be associated with several metrics factors to help determine the level of risk value related to a specific element or process. Risk is defined as the combination of the probability of occurrence and the consequences of a given future undesirable event. Risk can be associated with products and/or projects.

The determination of risk or vulnerability can be expressed as a function of:

- The likelihood (probability) of a given finding posing a risk to system development or functionality
- The magnitude of the impact of a finding posing a risk to system development or functionality

Where:

P = Probability
I = Impact
and: P x I = Risk Score

To measure risk, a risk scale and a risk-level matrix has been developed.

D.2 RISK DETERMINATION

Table D-1 displays the Risk Scale and required actions. This risk scale, with its ratings of High, Moderate, and Low, represents the degree or level of risk to which a system, facility, or procedure might be exposed to a given vulnerability were exercised. The risk scale also presents actions that senior management, the mission owners, must take for each risk level.

Table D-1 Risk Scale and Necessary Actions

Risk Rating	Action Implementation
High	High-risk levels create a strong need for corrective actions and the creation of an action plan that is put in place as quickly as possible.

Risk Rating	Action Implementation
Moderate	Moderate-risk levels warrant corrective actions and a plan to incorporate those actions within a reasonable period of time.
Low	For low-risk levels, the application owner must decide whether corrective actions are needed or whether the risks may be accepted.

D.3 RISK MITIGATION AND RECOMMENDATIONS

During the risk mitigation process, controls that could mitigate or eliminate the identified risks are provided. The goal of the recommended controls is to reduce the level of risk to FMPS and its data to an acceptable level. The following factors should be considered in recommending controls and alternative solutions to minimize or eliminate identified risks:

- Effectiveness of recommended options (e.g., system compatibility)
- Organizational policy
- Operational impact

For consistency and clarity and to maintain an accurate understanding of risk findings, IV&V adopted the CMS risk management methodology, as defined in the Risk Management Plan (CMS RMP – '*CMS Health Insurance Exchange Risk Management Plan v 1.1_04302012_Draft'*); accordingly, risks identified on the FFE project level will be shared with partner and stakeholder groups for visibility and shared understanding of FMPS project risks to support successful risk management at the project level and through the enterprise level through correlation to the FFE Integrated Master Schedule (IMS) milestones and tasks. The intent is to identify and appropriately address and elevate project risks to the Health Insurance Exchange Program level for visibility, mitigation and for possible action.

Each risk is documented as fully as possible to include probability (likelihood), impact, risk value, system & scope assessment area and overall characteristic. As a part of the documentation of the risk, a nominal probability (likelihood) and impact rating on the risk finding was submitted and was mathematically factored to reach an overall risk value. See Tables 2-3, 2-4, and 2-5 for probability, impact and risk value guidance.

Table D-2 Probability Assessment Criteria

Level	Probability	Probability of Occurrence
5	Near Certainty	81-99%
4	Highly Likely	61-80%
3	Likely	41-60%

Level	Probability	Probability of Occurrence
2	Low	21-40%
1	Not Likely	5-20%

Table D-3 Impact Assessment Criteria

Level	Impact
5	Severe degradation in technical threshold performance; jeopardizes project success. Cannot meet key milestones. Represented as a 20% deviation of the baselined plan.
4	Significant degradation in tech performance, unacceptably below goals, no design margins. Requires program or project critical path change. Represented as a 15–20% deviation of the baselined plan.
3	Moderate shortfall in tech performance, with limited impact; technical goals unmet and design margins significantly reduced. Schedule slip impacts milestone (MS) or Critical path slack. Represented as a 10–15% deviation of the baselined plan.
2	Minor reduction in technical performance, but can be tolerated, little impact; goals and design margins reduced. Schedule slip but will meet MS. Represented as a 5–10% deviation of the baselined plan.
1	Minimal consequence to performance, but no overall impact; goals and design margins will be met. No schedule slip. < 1% increase from baseline.

Table D-4 Risk Value

Risk Value Exposure Score	Risk Level
15-25	High
6-14	Moderate
1-5	Low

Exhibit 15

CGI. Monthly Status Report. Undated. Agenda # 3.

—MEETING MINUTES—

Subject:	FFE Monthly Contracts Status – March	**Participants (check if in person or on phone)**			
Person in charge of meeting:	Paul Weiss (CMS)	Paul Weiss (CMS)	√	[redacted] (CGI)	√
		Monique Outerbridge (CMS)	√	[redacted] (CGI)	√
Date:	3/27/2013	Lyandra Emmanuel (CMS)	√	[redacted] (CGI)	√
Start/finish time:	2:00pm – 3:00pm	Carolyn Robinson (CMS)	√	[redacted] (CGI)	√
Location:	Baltimore	Mark Oh (CMS)	√	[redacted] (CGI)	√
Venue:	CMS N3-20-01	Hung Van (CMS)	√		
		Allisan Hafner (CMS)	√		
		Star Blondell	√		
		Mickie Lewis	√		

1. Agenda Topics

#	Agenda / Discussion	Update provided

Confidential and Proprietary Data. Use of the data contained herein is subject to CGI Federal restrictions and applicable Federal Acquisition Data Rights Clauses

Contains Sensitive and Proprietary Business Information - Maintain as Confidential CGISFN100100974

#	Agenda / Discussion	Update provided
1.	General Topics	• CGI was informed that Hung Van will be the new GTL for the FFE contract. This is effective immediately. There is no need to change the task order to reflect this change since only the Project Officer is identified.
2.	Monthly Financial Status Report	• The February report was distributed via email prior to the meeting. • There was discussion over the high burn rate for the month of February, CGI explained that was due to Plan Management go-live activities and was anticipated. • CGI re-confirmed that funding will run out mid to late April.

3.	Business Area Topics (E&E/Plan Management, Financial Management, and Quality)	• CMS expects to be issuing a change request being driven by the White House's desire to extend the QHP window for re-submissions.
		• CMS wants confirmation that keeping USP Category Class Service up past 3/28 does not constitute a change in scope.
		  ○ CGI will confirm if O&M in the option period will cover underlying reference data updates. CGI also needs to verify the frequency of the reference data updates.
		  ○ There is an assumption that USP will not have any releases or enhancements.
		• USP Production Issue
		  ○ CGI and CMS discussed a recent issue related to an Out of Memory error versus Memory Leak problems was had; USP was getting an Out of Memory error which does not necessarily lead to a Memory leak problem.
		  ○ CMS suggested that CGI remove the nightly reboot scripts after 3/28 once USP goes down
		  ○ CMS also suggested that CGI conduct performance testing after 3/28 to determine if performance was a factor.

4.	IV&V Results	• CGI has reviewed the IV&V findings and will set up a meeting with appropriate CMS staff to discuss the next course of action for each finding. • An issue was identified and characterized as "bad code". As discussed with CMS, the label of "bad code" is correct. The error was coming from the Layer 7 policies and intermittent issues with Layer 7 software and not the FFE code. The ACA testing vendor also reported issues in the software which can be tracked back to the Layer 7 issues.

Confidential and Proprietary Data. Use of the data contained herein is subject to CGI Federal restrictions and applicable Federal Acquisition Data Rights Clauses

Contains Sensitive and Proprietary Business Information - Maintain as Confidential CGISEN100100975

#	Agenda / Discussion	Update provided
5.	Hours Allocation	• CGI reviewed the hours allocation spreadsheet with CMS. This spreadsheet will be used to track the budgeted hours by function for thie FFE project. CMS and CGI will use this tool to manage trade-off as changes or additional requirements are identified. o CGI and CMS will review the hours allocation spreadsheet bi-weekly; 1 at the monthly meeting at the beginning of the month and 2nd a the monthly contracts meeting o CGI will revise the legend on the spreadsheet to indicate that remaining hours allocation is based on currently "projected" funding which includes the pending modification. o CMS will review and validate the hours allocation based on functionality that CMS had identified as necessary for day-one. • Hardware Re-allocation o Approximately $1M of estimated Hardware costs will not be spent due to delayed activations and reduced Terremark rates; CGI will reallocate this amount rto labor costs
6.	Missed Dates Report	• CGI distributed the Missed Dates Report for discussion. Several PM requirements have been closed and are no longer on the list. CGI added E&E requirements due dates which have been missed.
7.	Risks and Issues	• Integration Risk with other software/vendors and dependent programs such as EIDM is the biggest risk with everything going live at the same time. • Late findings on the SCA testing is resulting in last minute software changes. Therefore there is not enough time remaining for thorough testing for fix. CGI received direction for one of the findings to not allow 'xls' documents on uploads to supplemental documents. • CGI suggested holding a lessons learned session sometime in April/May with all contractors involved with the Plan Management deployment

2. Action Items

#	Description	Assigned to	Status Date – Status – Comments	Due Date

Confidential and Proprietary Data. Use of the data contained herein is subject to CGI Federal restrictions and applicable Federal Acquisition Data Rights Clauses

Contains Sensitive and Proprietary Business Information - Maintain as Confidential CGISEN100100976

Exhibit 16

CGI. Proposed Change Request. April 15, 2013.

From: Oh, Mark U. (CMS/OIS) [redacted]
Sent: Thursday, April 18, 2013 9:22 AM
To: [redacted] (CGI Federal); [redacted] (CGI Federal); [redacted] (CGI Federal); [redacted]
Cc: Van, Hung B. (CMS/OIS)
Subject: ROM for PRA related work
Importance: High

Hi [redacted] – per discussion from yesterday, the highlighted CRs (#3, #4.g, #5) will not be pursued. With that said, we need ROM for remainder of the items. We have a meeting with CCIIO and need to understand ROM (not from contractual sense but from program estimation sense) for these items. Can you send us the ROM COB today or first thing tomorrow morning? Do you want us to set-up a quick call to jointly draft ROM?

CR # and Summary	Priority (as reported)	Disposition Summary (from OIS Review)
CR #1: ESC and non-ESC MEC Modifications (four components)	High	All components of CR #1 is possible to implement by Day 1 1.1: Assumes no changes to the existing non-ESC MEC eligibility logic
CR #2: Prospective Loss of non-ESC-MEC	High	CR #2 is possible to implement by Day 1
CR #3: Incomplete application handling (securing Medicaid/CHIP date)	High	**CR #3 is Not feasible to be implemented by Day 1.** Due to the high impact on the existing application UI and logic, this CR is not feasible for Day 1 implementation.
CR #4.a: Income Discrepancies (new questions)	High	CR #4.a is possible to implement by Day 1
CR #4.b: New Section - Collect Navigator, Agent/Broker and other assister information	High	CR #4.a is possible to implement by Day 1
CR #4.c: Build Household- Immigration Status changes to document types and data fields	High	CR #4.a is possible to implement by Day 1
CR #4.d: Household Contact preferences changes to contact methods questions	Medium	CR #4.a is possible to implement by Day 1
CR #4.e: Income Screener Change	Medium	CR #4.a is possible to implement by Day 1
CR #4.f: Authorized Representative	Medium	CR #4.a is possible to implement by Day 1

Contains Sensitive and Proprietary Business Information - Maintain as Confidential CGISEN100100056

CR #4.g: Build household – Auto-populate Name of individual for claiming tax filer	High	**CR #4.g is Recommend Closure.**
CR #5: Early Medicaid Check	High	**CR #5 is Recommend Closure.** Though it is possible to implement by Day 1, this change not necessary for Day 1.

Contains Sensitive and Proprietary Business Information - Maintain as Confidential

Proposed Change Requests from E&E – 4-15-13

The below CRs are changes that need final resolution by this Friday (4/19)

Title	Description	Affected Functionality	Priority	Resolution Date and Next Steps	Risk
CR #1 ESC and non-ESC MEC Modifications	These changes stem from WH input on the application and are necessary to align front-end design of application with back-end design. They include: 1) Change list of available options for questions about eligibility and enrollment in non-ESC MEC (eg add new options for TRICARE, move Medicare from one question to the other) 2) Ask individuals who have jobs and are members of the tax household for APTC eligible individuals for employer contact information (name, address, phone, EIN, secondary contact, phone, and email) .; 3) Reinstate follow-up questions and logic for handling retirees or former employees about their coverage, including logic, because COBRA and retiree coverage impacts the routing of an individual through the application; and 4) Simplify the questions related to whether the employee expects the employer to change coverage options by removing answers ("the amount paid for premiums for this plan will change" and "the frequency when [FNLNS] will pay this amount will change") and adding field to collect the date of each change.	Eligibility Logic Application Flow	High	Need resolution before questionnaire is finalized 4/19 Next steps – need LOE from OIS/CGI. To CCB this Wednesday.	Not addressing White House input.

Contains Sensitive and Proprietary Business Information - Maintain as Confidential

Exhibit 17

Sylvia Matthews Burwell. Nominee for Secretary of HHS. Responses to Questions for the Record. May 18, 2014. Delivered to the Committee on Health, Education, Labor, and Pensions.

exchanges have accurate, easily accessible information about which drugs are covered, which doctors are covered, and how much they cost?

Answer: I am committed to ensuring that HealthCare.gov provides the key information consumers need to make an informed selection from among the plans available to them. The Affordable Care Act requires that each plan in the Marketplace include a Summary of Benefits and Coverage and a link to the plan brochure, where consumers can learn more about which services are covered. If confirmed, I look forward to working with you to find ways to expand consumer access to information in an affordable manner.

4. **PPACA creates a 90-day grace period for individuals with subsidized coverage to pay their premiums before they are fully removed from their insurance. Patients are considered covered for this entire 90-day period, but insurers are only required to pay claims incurred in the first 30 days. That leaves a 60-day gap in which people are accessing health care services and incurring costs for which they may have no intention to pay. Who will pay the providers for the treatments that patients receive during this 60-day period?**

Answer: I understand that the Affordable Care Act provides individuals receiving a tax credit a three-month grace period to pay any unpaid premiums. This only applies to individuals who have already paid their first month's premium in full. The rules governing the grace period require plans to notify providers of the possibility for denied claims when an enrollee is in the second and third months of the grace period. If confirmed, I look forward to working with plans and providers to make sure the grace period is implemented in a way to reduce adverse effects to plans, providers, and consumers.

5. **What has been the total cost of creating healthcare.gov to date? What has been the total cost of "fixing" healthcare.gov? Please include a detailed accounting of all costs associated with this website, including (but not limited to) salaries and expenditures, contractor costs, and training.**

Answer: It is my understanding that as of February 28, 2014, CMS has obligated a total of approximately $834 million on Marketplace-related IT contracts and interagency agreements. These expenditures include the website and the systems that support enrollment through the Marketplace, such as the data services hub as well as other supporting IT infrastructure, including cloud computing, to support Marketplace IT development.

6. **What financial outlays are expected for fixing the backend of healthcare.gov? Please include a detailed estimate of future costs for fixing and maintaining the website, including (but not limited to) salaries and expenditures, contractor costs, and training.**

Answer: The President's Budget reflects a need for approximately $200 million for all Marketplace-related IT in FY 2015, some of which is funded through user fees. Much of this amount reflects ongoing operational and maintenance costs of HealthCare.gov, as well as continued development.

Exhibit 18

CGI. Response of CGI Federal Inc. to Additional Questions for the Record and Member Requests for the Record. Dec. 3, 2013. Obtained by House Energy & Commerce Committee.

Wiley Rein LLP

1776 K STREET NW
WASHINGTON, DC 20006
PHONE 202.719.7000
FAX 202.719.7049

7925 JONES BRANCH DRIVE
MCLEAN, VA 22102
PHONE 703.905.2800
FAX 703.905.2820

www.wileyrein.com

December 3, 2013

Robert L. Walker
202.719.7585
rlwalker@wileyrein.com

VIA E-MAIL

The Honorable Fred Upton, Chairman
Committee on Energy and Commerce
United States House of Representatives
2125 Rayburn House Office Building
Washington D.C. 20515-6115

Re: *Response of CGI Federal Inc. to Additional Questions for the Record and Member Requests for the Record*

Dear Chairman Upton:

Attached please find CGI Federal Inc.'s Responses to the Additional Questions for the Record and Member Requests for the Record set forth in the Committee's November 18, 2013 letter addressed to Cheryl Campbell, CGI Federal Inc. Senior Vice President. Please do not hesitate to contact me if you have any questions about the Attachments.

Sincerely,

Robert L. Walker

Attachment 1 – CGI Federal Inc. Responses to Additional Questions for the Record
Attachment 2 – CGI Federal Inc. Responses to Member Requests for the Record

cc: The Honorable Henry Waxman
Ranking Member

Attachment 1 – CGI Federal Inc. Responses to Additional Questions for the Record

The Honorable Joseph R. Pitts

1. In 1303(b)(3)(A) the Affordable Care Act specifies that "A qualified health plan that provides for coverage of the services described in paragraph (I)(B)(i) [abortion in cases other than rape, incest, or to save the life of the mother], shall provide a notice to enrollees, only as part of the summary of benefits and coverage explanation, at the time of enrollment, of such coverage." Please describe how the federally facilitated exchange website provides this abortion notice to enrollees.

As specified in the quoted passage of the Affordable Care Act, the law tasks qualified health plans with the responsibility for providing a notice of abortion coverage, but only as part of the summary of benefits and coverage explanation. Summaries of benefits and coverage explanations, which would include any notice to enrollees of the specified abortion coverage, are drafted by qualified health plans alone. The Federally Facility Marketplace ("FFM") provides links to the issuer-created summaries of benefits and coverage explanations within the interfaces for consumers to compare and select qualified health plans.

2. For those Americans who have been able to create an account and view plans on the federally facilitated exchanges, it has become evident that it is very difficult to ascertain whether a plan includes abortion coverage.

> **a. If a law were enacted to require that plans prominently display whether the plan includes abortion, how long would it take to make the necessary technical adjustments to comply?**
>
> **b. If a law were enacted to require that plans that include elective abortion disclose and identify separately the cost of the abortion surcharge described in section 1303(2)(B)(i)(II) every time the price of the plan is displayed, how long would it take to make the necessary technical adjustments to comply?**

The extent of the technical work required to comply with any future law requiring a change in the display of coverage for abortion or requiring separate identification of the cost attributable to that coverage would depend on a number of factors, including, but not limited to: the way in which such a law were interpreted and implemented by the Department of Health and Human Services ("HHS") and the Centers of Medicare & Medicaid Services ("CMS") regulations; whether the implementation of the laws would require collection and verification of additional information from each plan issuer; the availability of CMS personnel to design and define the content to comply; and the availability of other resources to support the effort. Generally, CGI Federal believes that the technical aspects of the changes discussed in this question could be accomplished through a relatively short-term effort.

<u>The Honorable Michael C. Burgess</u>

1. We have heard that various companies, contractors, insurers, etc. had daily contact with CMS just prior to launch. What was your experience in this regard?

> **a. Would you say your contact with CMS should have started earlier? Or maybe more to the point, should your contracts been awarded earlier giving you more time to work on these issues?**
>
> **b. Would you say that you were given tight or unrealistic deadlines in development?**
>
> **c. We have also heard that "to address lists" of problems of various severity levels were created. Was that your experience?**
>
> > **i. Were you aware of identified issues still unresolved on October 1?**
>
> **d. If the Administration had shared more information with you would you have been able to recognize that there was going to be a problem? Or did you say in fact, this is going to be a problem? If so to whom?**

As noted in Ms. Campbell's October 10, 2013 responses to earlier questions for the record from the Committee, CGI Federal's project team has been in regular, if not daily, contact with both CMS and other stakeholders around all aspects of the FFM since the first day of contract performance. CGI Federal has worked collaboratively throughout the course of the contract with CMS and with the other relevant stakeholders on development and implementation of the FFM and HealthCare.gov.

With respect both to the unique, complex nature of the FFM and to the initial timeframe available for completion of the FFM, the FFM has been characterized as a five-year project compressed into two years. This short schedule combined with other factors (such as delays in the identification and finalization of requirements, changes in direction on the design and development of user interfaces, and the required use of database technology that had never previously been deployed in a similar consumer facing way, among others) directly influenced CGI Federal's ability to meet the immovable October 1 "go live" date and resulted in constant re-prioritization of project tasks by CMS and severe compression of the timeframes available to complete those tasks. For these reasons, Ms. Campbell stated during her October 24 testimony that any additional time for development and testing would have been beneficial for a system as complicated as the FFM.

CGI Federal is not familiar with the term "to address lists;" however, prioritized lists of defects and issues of various severity levels analyzed and addressed by CGI Federal with CMS were created throughout the development of the FFM. Throughout performance of the FFM Task Order, CGI Federal advised CMS of concerns and risks it identified for the launch of this unique, complex system and endeavored with CMS to resolve or mitigate those risks and concerns to the extent possible. Although CGI Federal certainly was aware of identified issues with HealthCare.gov and the FFM component not yet resolved as of October 1, CGI Federal delivered a functional FFM as directed by CMS on the launch date and has continued since then, as planned and as expected with any application development and implementation project, to address outstanding issues in consultation with CMS.

2. When the website went live on October 1, did you feel you had submitted your best work?

a. Where [sic] you confident things would work or were you waiving red flags?

b. Were you working up against an unrealistic deadline and told to hand in whatever work you had done?

As Ms. Campbell testified on September 10, CGI Federal was optimistic that it would be able to deliver the functionality that CMS directed to enable qualified individuals to begin enrolling in coverage when the FFM went live on October 1. Throughout performance of the FFM Task Order, CGI Federal advised CMS of concerns and risks it identified for the launch of the unique and complex FFM application and tried, along with CMS, to resolve or mitigate those risks and concerns to the extent possible under the circumstances, including CMS' prioritization of critical, consumer-oriented functionality for launch. The FFM functioned at launch; clearly, however, performance issues surfaced and there remains work to be done. CGI Federal continues to resolve issues and develop new modules and functionality to fulfill CMS' objectives.

In further response to this question, CGI Federal references its response to Congressman Burgess' Question 1 above.

3. Based on what you know, how extensive are the problems with healthcare.gov?

a. Will the entire system have to re-built? Or can small integrated fixes address the problems?

b. Is the November 30 deadline set by HHS to fix all of the issues realistic?

As stated during Ms. Campbell's October 24 testimony, CGI Federal does not believe that it is necessary to re-build the FFM. Since October 1, CGI Federal has dedicated significant effort, in coordination with CMS and other stakeholders, to improving the FFM through optimization, tuning, and software releases to allow consumers to enroll at a faster pace and, overall, enjoy a smoother experience. As recently as December 1, 2013, CMS and Administration (*i.e.*, White House) officials have acknowledged publicly the significant improvements to the FFM since October 1 and CGI Federal has played a key role in delivering these system improvements.

Specifically, with respect to the improved performance, reliability, and stability of the FFM and HealthCare.gov as of November 30, the Administration's Jeffrey Zients told reporters on December 1: "[w]e have a much more stable system that's reliably open for business;" "HealthCare.gov can now support intended volumes." In addition, Secretary Sebelius wrote in a December 1 piece in *USA Today*:

> [W]e've been working 24/7 to make improvements, and more consumers are successfully shopping online and enrolling in a health plan each week. As a result, today's user experience on HealthCare.gov is a dramatic improvement over where it was on Oct. 1. The site is running faster, it's responding quicker and it can handle larger amounts of traffic. Now, there will be exceptions, and (as with any website) we will continue to make improvements. But the system is now working smoothly for the vast majority of users.

Although the November 30 deadline has passed, CGI Federal remains dedicated to supporting the mission of continuing to further improve and optimize the performance, reliability, and stability of the FFM and HealthCare.gov.

4. While we have heard a lot about the front end problems—like creating an account—isn't it true we may not even know the depth of other problems that may come as consumers continue upstream?

a. What problems do you anticipate in the next few months as more users access the website and attempt to actually sign up for plans?

b. Are you in contact with CMS about any of your future concerns?

Since the October 1 launch, CGI Federal has implemented fixes to the FFM application to address issues made apparent by the increasing availability and capacity of HealthCare.gov and the associated expanded user base. CGI Federal is working side by side with CMS and CMS' new "enhanced testing and integration contractor" for HealthCare.gov, Quality Software Systems, Inc. ("QSSI"), to anticipate and address future concerns. As part of this collective effort, CGI Federal endeavors to identify proactively issues: (1) around system performance and responsiveness likely to occur as more and more users access HealthCare.gov—including the FFM—between today and the end of open enrollment and (2) related to bringing additional functionality online to serve enrollees, CMS, states, issuers, and other FFM stakeholders. With a system as unique and complex as FFM, unanticipated problems will arise; CGI Federal is dedicated to working as part of the CMS team to resolve issues and continue to further improve the FFM application.

<u>The Honorable Leonard Lance</u>

1. Briefly, would you please walk through a normal process for creating and testing these systems? Do you have an average timeframe for building and performing end-to-end testing of these systems? What timeframe were you given to create and produce this system? When were you awarded the contract and when did you begin building the system? In the three years between enactment and October 1, 2013, when did you win the contract and begin building? Do you feel you were allowed adequate time to test a system of this magnitude?

The FFM is a first-of-its-kind system unique to CMS that was required to be conceptualized, defined, developed, tested, and launched with extreme urgency against the immovable deadline of October 1, 2013. CMS awarded the FFM Task Order to CGI Federal on September 30, 2011, providing a two-year time period for requirements definition, creation, production, and testing of the FFM application. During this time period, CGI Federal adhered to the CMS-controlled process for creating and testing the FFM. As stated by Ms. Campbell during her October 24 testimony, for a system as complicated as the FFM, any additional time for development and testing would have been beneficial.

2. Who made the decision to put the plan and cost information deep in the site?

a. Over the past few years, the Administration has been touting healthcare.gov as an easy, one-stop shop similar to amazon.com. In your opinion, why would they prohibit individuals from anonymously browsing plans and options before entering sensitive, personal information?

The design and content of the FFM is driven and maintained by CMS based on its determination of a logical workflow. To CGI Federal's understanding, CMS' business logic was dependent on the inherently customized nature of healthcare plans and costs, which dictate that particular information be obtained from applicants and computed before appropriate plan options and accurate cost information can be displayed. CGI Federal is not aware of involvement by the Administration (*i.e.*, White House) in decisions related to anonymous browsing.

3. In your professional opinion, what do you believe the best course of action would be to fix this without hurting the consumers who have already signed up?

a. What would it take to scrap the site and start over? Please elaborate in terms of time, manpower, and cost to the taxpayer.

As stated during Ms. Campbell's October 24 testimony, CGI Federal does not believe that it is necessary to re-build the FFM. CGI Federal will continue to dedicate its resources, in coordination with CMS and other stakeholders, to improve continuously the FFM to allow consumers to enroll at a faster pace and, overall, enjoy a smoother experience. This "continuous improvement" approach for a complex system such as the FFM is an industry best practice. As recently as December 1, 2013, CMS and Administration (*i.e.*, White House) officials have acknowledged publicly the significant improvements to the FFM since October 1 and CGI Federal has played a key role in delivering these improvements. CGI Federal is dedicated to supporting the mission of improving the performance, reliability, and stability of the FFM and HealthCare.gov under its FFM Task Order.

<u>The Honorable Bill Cassidy</u>

1. In your testimony in front of the Committee on September 10, 2013, you stated in your written testimony that CGI was tasked to "design and develop a FFM (Federally-Facilitated Marketplace) that will perform the functions and business processes that CMS has identified in regulations and guidance issued pursuant to the PPACA". In addition, you stated that "[t]he FFM will serve as the 'front door' for consumers to fill out an online health insurance application, determine their eligibility for health insurance, and enroll in a qualified health plan. Yet, in your October 24th testimony, you stated that the enterprise identity management (EIDM) function, provided by another contractor, serves as the "front door" of the Federal Exchange. Most would consider whatever appears to the user when they go on the website to be the "front door" of the exchange. Is CGI responsible for creating the interface from healthcare.gov captured by the screen shots below? If so, please explain what caused the website to produce the interface.

CGI Federal is responsible for building the FFM application. These screen shots capture error pages produced by the FFM. However, it is not possible from the screen shots alone to explain what caused the errors displayed. Errors like the ones shown could be caused, for example, by: problems in CGI Federal's FFM application; the environment of servers hosted by another contractor; external databases that the FFM relies on for information; or integrations with other pieces of HealthCare.gov not supplied by CGI such as the Enterprise Identity Management System or the Data Services Hub.

<u>The Honorable Gus Bilirakis</u>

1. Did you or anyone in your company ever express to HHS or CMS that the website's launch should be delayed, or that the website might crash or have serious problems at launch?

CMS established October 1 as the launch date through regulation to coincide with the start of open enrollment. CGI Federal worked, and continues to work, at the direction of CMS. Throughout performance of the FFM Task Order, CGI Federal informed CMS of its concerns and the known risks associated with and mitigations for launching the FFM application on October 1, so that CMS, as the systems integrator, could assess FFM along with the other components of HealthCare.gov and determine the viability of the planned launch under the evolving circumstances.

Attachment 2 – CGI Federal Inc. Responses to Member Requests for the Record

During the hearing, Members asked you to provide information for the record. For your convenience, relevant excerpts from the hearing transcript regarding these requests are provided below.

The Honorable Marsha Blackburn

1. Would you please submit how much you have been paid to date? How much are you being paid on retainer or either to clear up?

As of November 27, 2013, CGI Federal has been paid $112,003,175.09 under the FFM Task Order No. HHSM-500-T0012. As of the date of the last modification to the FFM Task Order (Modification 08), the fully funded value of the FFM Task Order's Base Period from September 30, 2011 through February 28, 2014 is $197,516,424.85 (*see* Contract Line Item Number ("CLIN") 0001, which currently consists of approximately 61% labor and 39% hardware/software). The total FFM Task Order value, including three one-year Option Periods for Operations and Maintenance (*see* CLINs 0002, 0003, and 0004) and one 6-month Transition Out Option Period (*see* CLIN 0005), for potential performance through March 01, 2017 is $293,550,376.65 (which currently consists of approximately 51% labor and 49% hardware/software). To be clear, CMS has yet to exercise any of these Option Periods. In addition to the FFM Task Order, CMS awarded CGI Federal approximately $7.5 million in funding under Task Order No. HHSM-500-T007 for work on various CMS websites, including post-launch improvement work on HealthCare.gov.

2. Does your current system keep detailed error logs that can be referenced with the difficulties that are surrounding healthcare.gov? Would you please submit those?

CGI Federal has access to error logs. CGI Federal submits to the Committee that production of these logs would not be reasonably practicable. These logs capture a huge volume of information, including a substantial volume of non-error information. Further, the logs contain highly technical data that is effectively meaningless unless the reviewer has specialized knowledge of computer programming and the FFM application and can review each entry in the context in which it was logged. Accordingly, CGI Federal submits that these logs would have little, if any, utility for the Committee.

The Honorable John Dingell

1. What actions have you taken to fix the Web site after the October 1 launch?

As noted in Ms. Campbell's October 24 testimony, CGI Federal has seen improvements day over day in the FFM:

> We're continuing to run queries against our database. We're running – reviewing system logs. We're fine-tuning our servers. We are analyzing the code for anomalies. Every day we're seeing where we're finding challenge in the system and making those corrections, as you would with any system that goes – that will go live.

Since October 1, 2013, CGI Federal has worked on a 24x7 basis and has taken numerous actions, both broad based and specific, to improve the FFM and HealthCare.gov, including, but not limited to: (1) embracing the Government's "tech surge" by augmenting the CGI Federal staff (including the involvement of CGI's Global CIO and other senior CGI Federal executives on a daily basis) and by working closely, cooperatively, and collaboratively with other recommended external resources, such as the former White House Fellows; (2) addressing the issues related to identity management and authentication that impacted HealthCare.gov immediately following October 1, including by diverting its most capable resources from ongoing FFM tasks to exploring alternative solutions to the problem, even though this related to a component of HealthCare.gov that was not the responsibility of CGI Federal; (3) deploying more than 30 releases to correct software issues; and (4) and augmenting and reorienting its staff as directed.

2. What suggestions do you have for there to be changes and improvements in the way the website is being dealt with by the Federal Government and what changes would you deem useful in seeing to it that the matter goes forward as it can and should?

CGI Federal, CMS, QSSI, and other partners have been working collaboratively as one integrated team to ensure the ultimate success of HealthCare.gov. In the spirit of this collaboration, CGI Federal has worked, and will continue to work, closely with CMS to improve the FFM's performance, enhance the user experience, and facilitate consumer enrollment. Throughout this process, CGI Federal has recommended and will continue to recommend concrete steps to address problems with the FFM specifically and with HealthCare.gov generally.

<u>The Honorable John Shimkus</u>
1. Who made the "see plans first" change on the website just before launch?

As detailed in CGI Federal's response to the Committee's requests for information submitted on October 28, 2013, CMS personnel decided not to include "anonymous shopper" functionality in the October 1, 2013 roll-out of the FFM. Based on CGI Federal's review and analysis of information to date, it appears that Mark Oh, Monique Outerbridge, Henry Chao, and Robert Thurston were involved in that decision.

2. Who made the decision that if you are younger than 50, you would be quoted a 25 year old health policy?

Please see response to Question 3 below.

3. Who made the decision that if you are older than 50, you get quoted a 50 year old policy?

CGI Federal notes that the premium estimation tool, launched on October 10, 2013, which allows consumers to browse health plans without creating an account, is found on the "Learn" portion of HealthCare.gov. According to CMS officials, when it first went live, the tool could only sort consumers into two categories—one over 50 and one below 50. CGI Federal understands that the decision to divide consumers into these broad groups was a business

decision made by CMS officials assisted by another contractor. CGI Federal was not involved in the business decision regarding how the estimator tool quoted plan information to consumers.

The premium estimator tool is separate from the FFM application developed by CGI Federal. Consumers utilizing the FFM application to select plans are quoted tailored plan information after they submit their information to the site. Accordingly, consumers entering the FFM portion of HealthCare.gov are not divided into over 50/under 50 categories.

The Honorable Joseph R. Pitts

1. Have you or your companies prepared memorandums or summaries explaining where the problems are with healthcare.gov? If you [sic], would you please submit them?

As stated during Ms. Campbell's October 24 testimony, CGI Federal has provided information about the status of the FFM as part of its operations, but it has not prepared separate, formal, comprehensive memoranda or summaries of the issues with the FFM or HealthCare.gov. Additionally, CGI Federal has produced a substantial volume of documentation to this Committee detailing the routine communications CGI Federal has had with CMS regarding problems with HealthCare.gov. Those communications form part of CGI Federal's October 28, 2013 and November 8, 2013 document productions.

The Honorable Gene Green

1. After the fix of the registration gateway, are you encountering new problems? Will you give us a background on those problems?

CGI Federal has worked to identify and fix all issues with its software application as it would in any application project in the course of ongoing use and testing. Of course, many issues that have impacted the overall performance of the FFM are unrelated to the application developed by CGI Federal.

For example, since resolution of the registration gateway known as the Enterprise Identity Management ("EIDM") developed by another contractor, CGI Federal has identified that the non-physical (or virtualized) database on which the FFM application is built (as directed by CMS) and the underlying storage infrastructure for the FFM application have been significant causes of capacity issues and have affected the FFM's stability and performance. In response to this issue, CGI Federal has continued to assess the performance of the systems under loads and worked to make all reasonable adjustments to optimize the FFM. As to the storage infrastructure, significant outages at another contractor's data center, which are beyond CGI Federal's control, have hampered efforts to identify and resolve defects in the FFM.

Additionally, CGI Federal has encountered other significant problems that do not relate to CGI Federal's portion of HealthCare.gov. For example, several weeks ago, the principal issue with HealthCare.gov was an IRS batch process that was calling on the system every hour. More recently, the principal problem was an overloaded firewall in the data center, which is the responsibility of another contractor. Although CGI Federal did not cause these and many other issues, it has been actively working with CMS to rapidly diagnose and resolve these problems along with its FFM defect resolution.

The Honorable Greg Walden

1. Did you make any recommendations to CMS about the need for end-to-end testing to occur sooner than the last two weeks before the website went live? Please submit those recommendations.

As explained above, CGI Federal adhered to the CMS-controlled process for creating and testing the FFM. As Ms. Campbell testified on October 24, for a system as complicated as the FFM, any additional time for development and testing would have been beneficial. Additionally, CGI Federal previously produced numerous documents relating to testing and respectfully refers the Committee to those materials.

The Honorable G.K. Butterfield

1. Did the White House ever order your company to mask the sticker shock of Obamacare by disabling the anonymous shopper function?

As stated during Ms. Campbell's October 24 testimony, CGI Federal did not receive any order directly from the White House regarding the anonymous shopper function. As detailed in CGI Federal's response to the Committee's requests for information submitted on October 28, 2013, CGI Federal understands that CMS personnel decided not to include "anonymous shopper" functionality in the October 1, 2013 roll-out of the FFM.

The Honorable Mike Rogers

1. Are you currently making changes in code to improve the functionality of healthcare.gov?

Yes, this is an ongoing element to the continuous improvement approach to the FFM and HealthCare.gov. As stated during Ms. Campbell's October 24 testimony, CGI Federal has, among other efforts, been making changes in code to improve HealthCare.gov. Indeed, CGI Federal has worked virtually around the clock to address defects identified in the code for the FFM application and defect resolution remains a constant priority. As reflected in the December 1, 2013 report from HHS, CGI Federal has made significant progress in resolving issues in the FFM code, which have directly led to significant improvements in the HealthCare.gov experience for users.

2. How many organizational boundaries does a piece of data cross when the data hub is populating information?

Data in the FFM, CGI Federal's portion of HealthCare.gov, interacts with EIDM (the registration tool), the data hub, states, and insurance companies. CGI Federal respectfully refers the Committee to QSSI, the contractor responsible for building the data hub, for additional responsive information on the additional organizational boundaries that data crosses in the hub.

3. Was an end-to-end security test of the whole healthcare.gov system done during the security verification?

CGI Federal was responsible for developing the FFM application to meet applicable security requirements. CGI Federal was not responsible for, nor did it conduct, end-to-end security testing on HealthCare.gov. With respect to questions regarding end-to-end testing, CGI Federal respectfully refers the Committee to CMS and the contractor retained by CMS to conduct security testing.

4. What are you doing to secure healthcare.gov from advanced persistent cyber threats?

CGI Federal is not responsible for monitoring HealthCare.gov for advanced persistent cyber threats; CGI Federal understands that CMS' Exchange Operations Center ("XOC") and other security contractors perform this function for HealthCare.gov. CGI Federal, however, is responsible for selecting and incorporating a Content Delivery Network ("CDN") service for the FFM and ensuring that the CDN provides on-going and managed Intrusion Prevention Services and appropriate Web Application Firewalls for CMS-hosted content. CGI Federal selected Akamai Technologies, the worldwide, premier provider of CDN services, to provide the CDN and meet the associated security requirements.

Moreover, security of the FFM application has been and continues to be a top priority for CGI Federal. As identified previously to this Committee, CGI Federal's design for the FFM system adheres strictly to CMS standards for security and data transmission. Specifically, the FFM is designed to comply with applicable portions of the Federal Information Security Management Act ("FISMA"), the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the Health Information Technology for Economic and Clinical Health Act of 2009 ("HITECH"), and regulations implementing those statutes. The FFM also is designed to comply with HHS' Policy for Information Systems Security and Privacy, which establishes comprehensive IT security and privacy requirements for HHS' IT security programs and information systems. Further, although no data will be stored on any hardware owned or operated by CGI Federal, because CGI Federal is sensitive to the fact that the FFM will be used to collect personal health information and other sensitive information necessary for individuals to enroll in health care, it has spent considerable time and effort to design a system that complies with these requirements. In addition, CGI Federal has undergone an independent evaluation and test of its systems security program as part of its FFM Task Order requirements.

5. Who is the independent contractor who is doing security testing on healthcare.gov?

MITRE is CMS' independent security testing contractor for HealthCare.gov.

6. Did you red-team or security stress test healthcare.gov in the two weeks before the launch?

CGI Federal was not responsible for performing red-team security testing on HealthCare.gov. CGI Federal understands that the type of testing referenced in the question would most likely be the responsibility of MITRE, CMS' independent security tester.

7. What entity certifies the security of healthcare.gov on a daily ongoing basis? Does CMS or an independent contractor certify the security? If an independent contractor, who is that contractor?

As stated during Ms. Campbell's October 24 testimony, CMS certifies the security of HealthCare.gov on an ongoing basis with the support of its independent security testing contractor, MITRE. Additionally, continuous monitoring of attacks, threats, and traffic on HealthCare.gov falls to the XOC, as mentioned above in response to Question 4.

8. Are the system administrators for CGI security trained in spear phishing?

Yes. CGI Federal systems administrators receive security training on phishing, including spear phishing. Systems administrators receive annual training from CGI Federal and also are certified by CMS on a yearly basis.

The Honorable Phil Gingrey

1. Was there ever a point that CGI expressed doubt as to whether the updated requirements would affect your ability for a successful launch? Who did you share that information with?

As stated during Ms. Campbell's October 24 testimony, CGI Federal shared with CMS the risks associated with any changes implemented by each formal contract modification. HealthCare.gov is a first-of-its-kind system. Delays in establishment and finalization of requirements—which extended throughout 2012 and 2013—played an important role in the compression of the time available for the development and testing of the FFM. As early as August 2012, CGI Federal advised CMS that delays in finalizing requirements threatened the development timeline. Indeed, CGI Federal repeatedly raised concerns to CMS about late-arriving and changing requirements. Those warnings can be seen in monthly status reports already provided to the Committee. Nevertheless, despite the numerous delays, CGI Federal worked collaboratively with CMS to deliver a functional FFM on the planned October 1 launch date and has continued since then to address outstanding FFM issues in consultation with CMS.

The Honorable Steve Scalise

1. How many errors have you logged since you have been tracking the errors in the system?

To put this response in context, CGI Federal emphasizes the significant difference between "errors" or "exceptions" tracked in connection with operation of HealthCare.gov and "defects" in the FFM application. The number of errors tracked in HealthCare.gov far exceeds the number defects in the FFM application. For example, a single defect in the FFM application could result in the recording of thousands of identical errors in the tracking logs. As a result, a large number of tracked errors would not mean that a correspondingly large number of defects exists, or existed, in the FFM application or HealthCare.gov. With respect to these errors or exceptions, because of the great difficulty in separating error entries from non-error entries in the server logs, CGI Federal has not determined the total number of errors tracked to date. However, from October 1 through December 1, 2013, CGI Federal has tracked approximately 698 defects with

the FFM application. As of December 1, 2013, CGI Federal has resolved approximately 85% of these defects by deploying more than 30 software releases.

The Honorable Robert Latta

1. You have stated that you only had about two weeks to make sure the site was integrated. How much testing did you do on medicare.gov? Did they give you a time frame? What was testing like at that time? What is a sufficient time frame?

CGI Federal's initial involvement with Medicare.gov occurred more than a decade ago; therefore, it is difficult to provide specific information as to the time period for testing of that site. CGI Federal's more recent involvement with Medicare.gov concerned redesign of the website. This redesign was less extensive than development of the FFM application, but did involve longer testing periods than allowed for the FFM application and HealthCare.gov as a whole. CGI Federal reiterates that, given the size, complexity, and the number of stakeholders involved in HealthCare.gov, any additional time for testing would have been beneficial.

2. How much time were you given to test FederalReporting.gov?

FederalReporting.gov went live in September 2009. It underwent at least eight weeks of performance testing—both CGI Federal testing and group benchmark performance testing. CGI Federal notes that FederalReporting.gov had a much smaller functional and technical scope than the FFM and had no problems when it was launched, aside from a single unplanned outage.

The Honorable David McKinley

1. Was your contract cost-plus based or performance-based?

As noted in CGI Federal's second response to the Committee's request for information submitted on November 8, 2013, the FFM Task Order is a cost-reimbursable type task order. The CLIN 0001 Base Period for Design, Development and Implementation is cost-plus-fixed-fee and the CLIN 0002, 0003, and CLIN 0004 Option Periods for Operations and Maintenance and the CLIN 0005 Option Period for Transition Out are cost-plus-award-fee.

The Honorable Cory Gardner

1. The Administration announced that the best and brightest are coming in to fix healthcare.gov. What individuals or companies are coming in to fix the website?

CGI Federal has added numerous CGI and subcontract resources to the team as part of the "tech surge." Additionally, as detailed in CGI Federal's first response to the Committee's request for information submitted on October 28, 2013, the following individuals were recommended by Government officials to and were interviewed and retained by CGI Federal as independent consultants to help improve the system performance under the FFM Task Order: Gabriel Burt; Paul Smith; Brian Holcomb; Gregory Gershwin; and Michael Dickerson (who CGI Federal understands is now under contract with QSSI).

The Honorable Adam Kinzinger

1. If applicants were able to sign up easily, but the 834 forms were coming in with a high number of errors, the results could potentially be disastrous. Reports indicate that dependents are being incorrectly coded as spouses. Have you identified that specific problem as part of the overall issue? What are the categories of problems with the 834 forms?

CGI Federal has identified the household composition issue described in the question. CGI Federal has addressed the source of this issue in the individual application and continues to work to resolve this issue.

By way of illustration, other categories of 834 form issues include data mapping issues. Data mapping issues occur where enrollment data incorrectly populates 834 forms with respect to phone numbers, email addresses, and county codes. CGI Federal has worked to correct these data mapping issues and anticipates that, as of the date of this response, these issues will have been substantially resolved. A further example of a category of 834-related issues concerned the auto-cancel feature, which operates by canceling an old plan once a consumer enrolls in a new plan; this error prevented the accurate generation of 834 forms. CGI Federal has already identified and substantially resolved this problem. As an additional example, CGI Federal has identified that certain 834 forms could not be processed by issuers because they lacked an identification number, such as a Social Security number. (Note, under law, applicants are not required to submit their Social Security number when completing an application in the FFM.) CGI Federal has worked with QSSI and CMS to ensure that applications in which the applicant withholds his/her Social Security number are still given an identification number and can be processed by issuers.

The Honorable Bill Johnson

1. Your contract required your company to deliver a risk management plan? Have you delivered that plan? Please provide the committee with a copy.

CGI Federal provided a copy of the risk management plan (at Bates numbers CGIHR00002370-2451) in its first response to the Committee's request for information on October 28, 2013.

The Honorable Renee Ellmers

1. How many individuals are now enrolled in health care coverage from the Web site?

CGI Federal respectfully refers the Committee to the Department of Health and Human Services for the number of individuals that have enrolled in health care coverage via HealthCare.gov.

Exhibit 19

CGI. Integrated FFM Schedule. June 28, 2013.

From: Schneer, Seth H. (CMS/CCIIO) [seth.schneer@cms.hhs.gov]
Sent: Monday, July 01, 2013 11:43 AM
To: [redacted] (CGI Federal); Thompson, Tyrone (CMS/OIS)
CC: Oh, Mark U. (CMS/OIS); [redacted] (CGI Federal); [redacted] (CGI Federal); 'lbjones@mitre.org' (lbjones@mitre.org); Van, Hung B. (CMS/OIS); [redacted] (CGI Federal); Jenkins, Michelle L. (CMS/OIS); [redacted] (CGI Federal); Webber, JoAnn (CMS/OIS); Henry, Galina (CMS/OIS); Chao, Bing (CMS/OIS); Mageras, Nicholas [USA] (mageras_nicholas@bah.com) (mageras_nicholas@bah.com); [redacted] (CGI Federal), stuart.grant@genovatech.com; FFE CCIIO Communications; [redacted] (CGI Federal); [redacted] (CGI Federal); [redacted] (CGI Federal); [redacted] (CGI Federal); [redacted] (CGI Federal); Alvarez, Carlos (CMS/OIS); Dunick, Walter T. (CMS/OIS); Lazenby, Daniel (CMS/OIS); polise_anthony@bah.com; Donohoe, Paul X. (CMS/OIS); Lewis, Angela [USA] (Lewis_Angela@bah.com); Suk, Grace K. (CMS/OIS); [redacted] (CGI Federal); [redacted] (CGI Federal); Mohs, Dean F. (CMS/CCIIO); Suk, Grace K. (CMS/OIS); Luan Nguyen (luan.nguyen@relis-llc.com); [redacted] (CGI Federal); Amos, Robert E. (CMS/OC); Duve, Rebecca J. (CMS/CTR); 'Hase, Jason' (Jason.Hase@noblis.org); Rowen, Stanley [USA]; [redacted] (CGI Federal); Hoang, Teresa [USA]; Mcveigh, Colin T. (CMS/CCIIO); [redacted] (CGI Federal); [redacted] (CGI Federal)
Subject: RE: Updated FFM Integrated Schedule

In the future, for your top line summary, can you please break out SHOP as a category separate from E&E?

It's difficult for us to track without it being broken out.

Thank you,

Seth

From: [redacted] (CGI Federal) [redacted]
Sent: Friday, June 28, 2013 11:55 PM
To: Thompson, Tyrone (CMS/OIS)
Cc: Oh, Mark U. (CMS/OIS); [redacted] (CGI Federal); [redacted] (CGI Federal); 'lbjones@mitre.org' (lbjones@mitre.org); Van, Hung B. (CMS/OIS); [redacted] (CGI Federal); Jenkins, Michelle L. (CMS/OIS); [redacted] (CGI Federal); Webber, JoAnn (CMS/OIS); Henry, Galina (CMS/OIS); Chao, Bing (CMS/OIS); Mageras, Nicholas [USA] (mageras_nicholas@bah.com) (mageras_nicholas@bah.com); [redacted] (CGI Federal); stuart.grant@genovatech.com; FFE CCIIO Communications; [redacted] (CGI Federal); [redacted] (CGI Federal); [redacted] (CGI Federal); [redacted] (CGI Federal); [redacted] (CGI Federal); Alvarez, Carlos (CMS/OIS); Dunick, Walter T. (CMS/OIS); Lazenby, Daniel (CMS/OIS); polise_anthony@bah.com; Donohoe, Paul X. (CMS/OIS); Lewis, Angela [USA] (Lewis_Angela@bah.com); Suk, Grace K. (CMS/OIS); [redacted] (CGI Federal); [redacted] (CGI Federal); Mohs, Dean F. (CMS/CCIIO); Schneer, Seth H. (CMS/CCIIO); Suk, Grace K. (CMS/OIS); Luan Nguyen (luan.nguyen@relis-llc.com); [redacted] (CGI Federal); Amos, Robert E. (CMS/OC); Duve, Rebecca J. (CMS/CTR); 'Hase, Jason' (Jason.Hase@noblis.org); Rowen, Stanley [USA]; [redacted] (CGI Federal); Hoang, Teresa [USA]; Mcveigh, Colin T. (CMS/CCIIO); [redacted] (CGI Federal); [redacted] (CGI Federal)
Subject: RE: Updated FFM Integrated Schedule

Contains Sensitive and Proprietary Business Information - Maintain as Confidential

Good Evening Tyrone –

Attached please find the integrated FFM schedule, updated with the current % complete for all active tasks.

We are currently tracking at approx. 41% complete, overall for tasks focused on Day 1 (October 1, 2013) functionality. As you know, this schedule does not include tasks previously completed prior to Sprint 15. Tasks currently at risk for on time completion are highlighted in RED, including some requirements which still need to be provided by Genova.. The breakout of the individual modules are:

Name	% Complete
FMM	41%
Eligibility and Enrollment	43%
Financial Management	14%
Plan Management	63%
Technical Architecture	46%
Infrastructure and Operational Readiness	24%

Please let me know if you have any questions or concerns. Have a great weekend.

Thank you,

[redacted]

CGI [redacted], PMP | Manager | CGI Federal – Health & Compliance
[redacted] | 593 Herndon Parkway, Herndon, VA | [redacted]

We cannot solve our problems with the same thinking we used when we created them. – Albert Einstein

CONFIDENTIALITY NOTICE: Proprietary/Confidential Information belonging to CGI Group Inc. and its affiliates may be contained in this message. If you are not a recipient indicated or intended in this message (or responsible for delivery of this message to such person), or you think for any reason that this message may have been addressed to you in error, you may not use or copy or deliver this message to anyone else. In such case, you should destroy this message and are asked to notify the sender by reply e-mail.

Please consider the environment before printing this email or its attachments.

Exhibit 20

Email from Lori Stone (CGI) to CMS officials. Updated FFM Integrated Schedule. Aug. 5, 2013. CGI100003683.

From: [redacted] (CGI Federal) [redacted]]
Sent: Monday, August 05, 2013 8:51 AM
To: Thompson, Tyrone (CMS/OIS) (tyrone.thompson2@cms.hhs.gov)
CC: Oh, Mark U. (CMS/OIS) (mark.oh@cms.hhs.gov); [redacted] (CGI Federal); [redacted]. [redacted] (CGI Federal); 'lbjones@mitre.org' (lbjones@mitre.org); Van, Hung B. (CMS/OIS) (Hung.Van@cms.hhs.gov); Jenkins, Michelle L. (CMS/OIS) (Michelle.Jenkins@cms.hhs.gov); [redacted] (CGI Federal); Webber, JoAnn (CMS/OIS) (JoAnn.Webber@cms.hhs.gov) (JoAnn.Webber@cms.hhs.gov); Henry, Galina (CMS/OIS) (Galina.Henry@cms.hhs.gov) (Galina.Henry@cms.hhs.gov); Bing Chao (Bing.Chao@cms.hhs.gov) (Bing.Chao@cms.hhs.gov); Mageras, Nicholas [USA] (mageras_nicholas@bah.com) (mageras_nicholas@bah.com); [redacted] (CGI Federal); stuart.grant@genovatech.com; FFE CCIIO Communications; [redacted] (CGI Federal); [redacted] (CGI Federal); [redacted] (CGI Federal); [redacted] (CGI Federal); [redacted] (CGI Federal); Alvarez, Carlos (CMS/OIS); Dunick, Walter T. (CMS/OIS); Lazenby, Daniel (CMS/OIS); polise_anthony@bah.com; Paul.Donohoe@cms.hhs.gov; Lewis, Angela [USA] (Lewis_Angela@bah.com); Grace.Suk@cms.hhs.gov; [redacted] (CGI Federal); [redacted] (CGI Federal); Mohs, Dean F. (CMS/CCIIO); Schneer, Seth H. (CMS/CCIIO); Grace.Suk@cms.hhs.gov; Luan Nguyen (luan.nguyen@relis-llc.com); [redacted] (CGI Federal); Amos, Robert E. (CMS/OC) (Robert.Amos@cms.hhs.gov); Duve, Rebecca J. (CMS/CTR) (Rebecca.Duve@cms.hhs.gov); 'Hase, Jason' (Jason.Hase@noblis.org); Rowen, Stanley [USA]; [redacted] (CGI Federal); Hoang, Teresa [USA]; colin.mcveigh@cms.hhs.gov; [redacted] (CGI Federal); Couts, Todd (CMS/OIS) (Todd.Couts1@cms.hhs.gov) (Todd.Couts1@cms.hhs.gov)
Subject: RE: Updated FFM Integrated Schedule
Attachments: FFM_IMS.zip

Good Morning Tyrone –

Attached please find the integrated FFM schedule, updated with the current % complete for all active tasks.

We are currently tracking at approx. 52% complete, overall for tasks focused on Day 1 (October 1, 2013) functionality. As you know, this schedule does not include tasks previously completed prior to Sprint 15. Tasks currently at risk for on time completion are highlighted in RED, including some requirements which still need to be provided by Genova. The breakout of the individual modules are:

Contains Sensitive and Proprietary Business Information -- Maintain as Confidential

Exhibit 21

Email from CGI to CMS. FFE12-010 FEPS-FFM Monthly Status Report – August2013. Table 6: Open Risks. Sept. 6, 2013.

From: [redacted] (CGI Federal) [[redacted]]
Sent: Friday, September 06, 2013 3:57 PM
To: '[redacted]; [redacted]; [redacted]
'Van, Hung B. (CMS/OIS)'; [redacted]; '[redacted]
CC: [redacted] (CGI Federal); [redacted] (CGI Federal); FFE CCIIO Communications
Subject: HHSM-500-2007-000151 Task Order HHSM-500-T0012 (Monthly Status Report for August 2013)
Attachments: FFE12-010 FEPS-FFM Monthly Status Report - August2013.docx

Hello,

Please find attached CGI's Monthly Status Report for August 2013.

Best regards,

[redacted]

[redacted] | Executive Consultant | CGI Federal | [redacted] | [redacted] | [redacted]

CONFIDENTIALITY NOTICE: Proprietary/Confidential Information belonging to CGI Group Inc. and its affiliates may be contained in this message. If you are not a recipient indicated or intended in this message (or responsible for delivery of this message to such person), or you think for any reason that this message may have been addressed to you in error, you may not use or copy or deliver this message to anyone else. In such case, you should destroy this message and are asked to notify the sender by reply e-mail.

Contains Sensitive and Proprietary Business Information -- Maintain as Confidential

Centers for Medicare & Medicaid Services
Center for Consumer Information and Insurance Oversight
7500 Security Blvd.
Baltimore, MD 21244-1850

FEPS - FFM
Monthly Project Status Report, Reporting Period – August 2013

Last Modified: AUTODATE

Document ID: FFE12-0010

Contract Number: HHSM-500-T0012

Contains Sensitive and Proprietary Business Information --
Maintain as Confidential

REVISION HISTORY

Version	Date	Organization/Point of Contact	Description of Changes
1.0	03/06/2013	CGI Federal	Baseline Template

495
Contains Sensitive and Proprietary Business Information -- Maintain as Confidential
CGIHR00024868

TABLE OF CONTENTS

1. Project Execution **1**

1.1. Significant Work Accomplished This Month 1
1.1.1. Deliverables 1
1.1.2. Upcoming Deliverables 2
1.1.3. Meetings 2
1.2. High Level Status by Work Stream 3
1.3. Upcoming Major Milestones 5
1.4. Project Dependencies – 30 Day Outlook 5
1.5. Open Risks 6
1.6. Open Issues 7

LIST OF TABLES

Table 1: Deliverables 1
Table 2: Pending Deliverables 2
Table 3: High Level Status by Work Stream 3
Table 4: Upcoming Major Milestones 5
Table 5: Project Dependencies 5
Table 6: Open Risks 6
Table 7: Open Issues 7

496
Contains Sensitive and Proprietary Business Information -- Maintain as Confidential
CGIHR00024869

1. Project Execution

1.1. Significant Work Accomplished This Month

1.1.1. Deliverables

Table 1 identifies the deliverables completed during the reporting period.

Table 1: Deliverables

Document Name	Delivery Date
HIX Configuration Management Plan August 2013	8/6/13
HIX Contingency Plan August 2013	8/6/13
HIX PIA August 2013	8/6/13
HIX E-Authentication Workbook August 2013	8/6/13
HIX Safeguard Procedures Report August 2013	8/6/13
Section 508 Product Assessment (EE)	8/9/13
Plan Preview User Guide	8/9/13
SRD/RTM (EE & PM)	8/15/13
System Design Document (EE & PM)	8/15/13
Interface Control Document (EE & PM)	8/15/13
Business Service Definition (EE)	8/15/13
User Guide (EE)	8/15/13
LCM /PCM (EE & PM)	8/15/13
Service Sequence Diagram (EE)	8/15/13
UI Specifications (EE)	8/15/13
Service Specifications (EE & PM)	8/15/13
Test Cases (EE & PM)	8/15/13
SoapUI Project (EE)	8/15/13
Draft Test Summary Report (EE & PM)	8/15/13
Defect Reports (Comprehensive and 508) (EE & PM)	8/15/13
Release Plan Report (EE)	8/15/13
508 PAT (EE & PM)	8/15/13
Release Notes	8/15/13
EVM Reports – July 2013	8/26/13
Draft SRD/RTM (EE & FM)	8/30/13
System Design Document (EE & FM)	8/30/13
User Guide (EE)	8/30/13
LCM/PCM (EE & FM)	8/30/13
O&M Manual (FM)	8/30/13
Service Sequence Diagrams (EE & FM)	8/30/13
Service Specifications (EE & FM)	8/30/13
Test Cases (EE)	8/30/13
SoapUI Project (EE)	8/30/13
Draft Test Summary Report (EE & FM)	8/30/13

Contains Sensitive and Proprietary Business Information -- Maintain as Confidential

CGIHR00024870

Document Name	Delivery Date
Defect Reports (Comprehensive and 508) (EE & FM)	8/30/13
Release Plan Report (EE & FM)	8/30/13
Release Notes	8/30/13

1.1.2. Upcoming Deliverables

Table 2 identifies the upcoming deliverables planned to CMS.

Table 2: Pending Deliverables

Document Name	Proposed Date
High Level Technical Design Document (Cross Module)	9/6/2013
System Requirements Document/Requirements Traceability Matrix (E&E and PM)	9/6/2013
System Design Document (E&E and PM)	9/6/2013
Interface Control Document (E&E)	9/6/2013
LCM (E&E and PM)	9/6/2013
PCM (E&E and PM)	9/6/2013
Gateway Service Specifications (E&E)	9/6/2013
Data Service Specifications (E&E and PM)	9/6/2013
Business Service Specifications (E&E and PM)	9/6/2013
Service Sequence Diagram (E&E and PM)	9/6/2013
UI Specifications (E&E and PM)	9/6/2013
User Guide (E&E, ESD and PM)	9/6/2013
Business Service Definition (E&E)	9/6/2013
Test Case (E&E and PM)	9/6/2013
Defect Report (E&E and PM)	9/6/2013
Test Summary Report (E&E and PM)	9/6/2013
508 PAT (E&E and PM)	TBD
Release Plan Report (E&E and PM)	9/6/2013
Release Notes (Cross Module)	9/6/2013
Day 1 Complete Documentation Package (E&E)	9/16/2013

1.1.3. Meetings

The various meetings CGI team members participate in during the month are discussed, in detail, during the FEPS Touch Base Calls.

Contains Sensitive and Proprietary Business Information -- Maintain as Confidential

CGIHR00024871

1.2. High Level Status by Work Stream

Table 3 provides a high level status overview of accomplishments, for each work stream, reflecting the current reporting period.

Table 3: High Level Status by Work Stream

Workstream	Status
Task Order Management	• Participated in weekly FFM and IPT Status meetings • Participated in daily status calls and ad hoc "Tiger Team" meetings • Attended monthly Contracts meeting • Prepared and delivered monthly EVM reports • Prepared and delivered Release documentation • Conducted Staffing/Recruiting in support of on-going work • Managed overall FFM Integrated Schedule • Managed project risks and issues and maintaining log • Implemented IQ Suite – daily task tracker and management-level status dashboards
Technical Solution Architecture & Ops Support	• Finalized design and detailed task plan for preparing the production environment for performance testing (prod prime) to commence on 09/16 and then the soft launch (merging prod prime, additional capacity, and current prod) to commence on 09/23 • Finalized the release schedule / build cadence and planned any additional dev/test/impl environment setup aligned to this plan • Supported the SCA to yield a successful audit; mitigated the 1 critical finding • Conducted internal performance testing; tuned configuration settings in multiple tiers; identified an Alfresco issue and will validate fix from software vendor in early Sep; identified longer running MarkLogic queries inside Plan Compare and will optimize in early Sep • Improved build and deployment processes • Improved process/tools for incident tracking and defect tracking • Worked with TWS team to set up all required Production jobs in TWS
Regional Technical Support & Training	• Delivered E&E and ESD 8/30 guide updates • Delivered first round of ESD training material to CMS • Prepared White House captivate demo • Facilitated Alpha Issuer calls and troubleshooting webinars • Liaison to CMS External testing PMO and teams • Began internal prep meetings for preparing IMPL1A for Issuers and States by 9/16 • Facilitated connectivity troubleshooting sessions with DSH and Issuers • Triaged Issuer reported defects/issues

Contains Sensitive and Proprietary Business Information -- Maintain as Confidential

CGIHR00024872

Workstream	Status
Operations & Maintenance	• Supported Help Desk • Conducted smoke and regression testing support for code plan preview and plan compare deployment • Conducted end to end testing support of EE module • Generated CALT/QC Reports • Team on loan to different pods (2xBA, 9xDev, 3xQA)
Help Desk	• Received and processed 1880+ tier two Help Desk Tickets during the month of August • Participated in weekly help desk calls with CMS CCIIO • Participated in daily triage calls with CMS OIS • Integrated IQ Suite into the help desk team • Provided IQ Suite overview training and revised internal help desk procedures • Participated in numerous triage calls to identify and resolve issuer challenges • Provided various reports in support of data calls for CMS
Plan Management	• Completed capture of 3,034 NAIC plans via Plan Transfer – SERFF. • Deployed Plan Transfer—OPM into Production, captured all 117 OPM plans. • Deployed Plan Preview for individual and SHOP into Production. • Developed Plan Preview defect fixes and implemented changes to support Dental plan requirements changes. • Supported Security Controls Assessment testing of Plan Preview; no findings reported by SCA testers. • Completed development of Ratifications, Certifications functionality.
Financial Management	• Delivered SBM & CSR Amount Calculation Functionality • Successfully processed NAIC-HI and DC SBM submission files in Production • Executed a total of 149 test cases and resolved 71 defects in total • Completed 75% of integration testing with OFM on HIGLAS Interface • Completed designs and kick-off development on APTC/CSR/XUF Functionality

E&E	• Successfully launched My Account Lite
	• Conducted significant development and testing in support of Oct 1 launch and future releases:
	  ○ Individual Application
	  ○ Enrollment
	  ○ Plan Compare
	  ○ ESD
	  ○ My Account
	  ○ Notices

Contains Sensitive and Proprietary Business Information -- Maintain as Confidential

CGIHR00024873

Workstream	Status
	○ Call Center Integration ○ Direct Enrollment ○ Account Transfer ○ SHOP • Integrated with Informatica • Successfully tested Direct Enrollment functionality with Issuers • Successfully tested Call Center APIs with NGD • Successfully sent 834 enrollment transactions to Issuers

1.3. Upcoming Major Milestones

Table 4 presents key milestones occurring during the next reporting period.

Table 4: Upcoming Major Milestones

Milestone	Due Date	Status
Operational Readiness Review	9/4/13	On track
Code Freeze for Day 1 Functionality	9/5/13	On track
Demo for White House	9/5/13	
Production Readiness Review	TBD	
Day 1 Deployment to Production	TBD	
Soft Launch	9/23/13	
Open Enrollment	10/1/13	

1.4. Project Dependencies – 30 Day Outlook

Table 5 presents high-level items on which CGI is dependent upon to begin key tasks in the work plan.

Table 5: Project Dependencies

Workstream	Dependency	Responsible Party	Due Date	Status
Business Architecture	Blueprint Baselining	BAH	Various	On Hold
Development	Business Requirements	CMS	See Project Schedule and Outstanding Requirements Report	In Progress
Development & Testing	Firewall Requests	URS	Various	In Progress

Contains Sensitive and Proprietary Business Information -- Maintain as Confidential

1.5. Open Risks

Table 6 presents the top risks currently open in the risk register.

Table 6: Open Risks

CALT ID	Title	Description	Date Opened	Risk Status	Probability & Priority	Impact	Mitigation Strategy
artf151840	Limited Testing Timeframes	The timeframes for testing in Dev and Test2 are not adequate to complete full functional, system, and integration testing activities.	8/9/2013	2-Open	5 - Near Certainty	4 - Significant	Work with CMS to establish a realistic schedule that will allow for the necessary testing.
artf151998	Revised requirements for interacting with EIDM/ Experian	Revised requirements for interacting with EIDM/Experian when interacting with FARS (for consumers who have called Experian and been manually ID Proofed) have been created, which will require EIDM to create an additional service (i.e., to fetch the FARS data for a consumer). The risk is that this CGI is dependent upon EIDM to create the service in a timeframe that will allow FFM to consume.	8/14/2013	2-Open	5 - Near Certainty	5 - Severe	Discuss with OIS regarding the priorities of these changes and if it can be postponed as post-Day 1.
artf151841	Plan preview allows issuers to only test ten predefined scenarios.	As directed by CMS, plan preview allows issuers to only test ten predefined scenarios. This covers a small subset of combinations of inputs, increasing the chances of missing data issues or system defects.	8/19/2013	2-Open	5 - Near Certainty	3 - Moderate	CGI will conduct testing beyond the 10 identified scenarios to the extent possible prior to Oct. 1.
artf151842	Informatica not installed in Test2 or Prod Prime	Informatica is required to conduct testing of Contact Information including, USPS Modals. Code requiring Informatica cannot be fully tested in the TEST2 and Prod Prime environments until Informatica is installed.	8/19/2013	3-Mitigation Implemented	4 - Highly Likely	4 - Significant	Work with MIDAS and IDL to get informatica installed and working in Test2 and Prod Prime. 8/28 - We have confirmed and tested the set up in test2. We'll be able to confirm in prod prime this weekend when we do the next deployment.

Contains Sensitive and Proprietary Business Information -- Maintain as Confidential CGIHR00024875

1.6. Open Issues

Table 7 presents the outstanding open issues currently being mitigated by the team.

Table 7: Open Issues

CALT ID	Title	Description	Date Opened	Status	Impact	Priority	Estimated Due Date	Corrective Action
artf151838	CGI does not have access to necessary tools to manage envs in test, imp, and prod.	CGI does not have access to necessary tools to manage envs in test, imp, and prod. Specifically (1) we don't have access to central log collection/view (2) we don't have access to monitoring tools. We have repeatedly asked CMS and URS but have not been granted this access.	6/5/2013	1-Open/New	5 - Severe	1 - Highest	6/28/2013	Provide access to existing tools that are operated by URS. We have requested this access but it has not been granted. 1. Document which tools we need, for which environments, and by when ([redacted] 6/18 2. [redacted] to request a weekly call with [redacted]) to discuss progress of monitoring. Communicate needs to [redacted] and explain implications of not having access. 3. [redacted] to take lead. [redacted] to request the meeting. 6/13
artf151837	Not Enough Time in Schedule to Conduct Adequate Performance Testing	Due to the compressed schedule, there is not enough time built in to allow for adequate performance testing.	8/9/2013	1-Open/New	3 - Moderate	1 - Highest	8/27/2013	Work with CMS to determine if any shifts can be made to allow for more time for performance testing.
artf151835	Hub Services are Intermittently Unavailable	Hub services are intermittently unavailable which affects FFM development and testing activities. This also impacts issuer testing in the Test2 environment.	8/13/2013	1-Open/New	4 - Significant	1 - Highest	8/29/2013	CGI Ops team will put a monitor in place (4-5 items) to alert whenever the Hub goes down. We will notify developers and the Hub so they are aware. We will log outage stats over time.
artf151839	Requests to support UAT	The CGI FFM QA team is receiving numerous emails, calls for demos, walk-throughs, questions, functionality requirements clarifications, environment setup, etc. directly from the CMS (OIS/CCIIO/OC) UAT users and staff bypassing the established ACA UAT vendor.	8/23/2013	1-Open/New	3 - Moderate	2 - High	8/23/2013	Clarify the UAT process with CMS and the ACA testing vendor's management, such that the CGI FFM QA team is not required to support UAT.

Contains Sensitive and Proprietary Business Information -- Maintain as Confidential CGIHR00024876

FEPS - FFM

CALT ID	Title	Description	Date Opened	Status	Impact	Priority	Estimated Due Date	Corrective Action
artf151999	EIDM - Reference Code Issue	FFM is not receiving the Reference Code as a response from the Submit User Info or the Modify User service. (Consequently, we cannot show the consumer the reference code to use when calling Experian to attempt to be manually ID Proofed). This impacts our ability to deliver the Manual ID Proofing items.	8/24/2013	1-Open/New	4 - Significant	2 - High	8/27/2013	EIDM needs to send the Reference Code as a response from the Submit User Info or the Modify User service.
artf151836	Lower Environments do not have required configurations in place	The lower environments are not configured with EIDM, Akamai, and sometimes required connectivity. Thus full integration testing cannot take place in these environments causing untested code to be promoted to higher environments.	8/9/2013	3-In Progress (Implementing Actions)	4 - Significant	1 - Highest	8/9/2013	1. Review list of existing integrations in all environments 2. Work with CMS to make a plan to address gaps 8/28 - Plan is currently being addressed based on priority.

Contains Sensitive and Proprietary Business Information – Maintain as Confidential CGIHR00024877

Exhibit 22

Email from CGI to CMS officials. Updated FFM Integrated Schedule. Aug. 17, 2013. CGI100007942.

From: [redacted] (CGI Federal) [redacted]
Sent: Saturday, August 17, 2013 4:45 PM
To: Thompson, Tyrone (CMS/OIS) (tyrone.thompson2@cms.hhs.gov)
CC: Oh, Mark U. (CMS/OIS) (mark.oh@cms.hhs.gov); [redacted] (CGI Federal); [redacted] (CGI Federal); 'lbjones@mitre.org' (lbjones@mitre.org); Van, Hung B. (CMS/OIS) (Hung.Van@cms.hhs.gov); Jenkins, Michelle L. (CMS/OIS) (Michelle.Jenkins@cms.hhs.gov); [redacted] (CGI Federal); Webber, JoAnn (CMS/OIS) (JoAnn.Webber@cms.hhs.gov) (JoAnn.Webber@cms.hhs.gov); Henry, Galina (CMS/OIS) (Galina.Henry@cms.hhs.gov) (Galina.Henry@cms.hhs.gov); Bing Chao (Bing.Chao@cms.hhs.gov) (Bing.Chao@cms.hhs.gov); Mageras, Nicholas [USA] (mageras_nicholas@bah.com) (mageras_nicholas@bah.com); [redacted] (CGI Federal); stuart.grant@genovatech.com; FFE CCIIO Communications; [redacted] (CGI Federal); [redacted] (CGI Federal); [redacted] (CGI Federal); [redacted] (CGI Federal); Alvarez, Carlos (CMS/OIS); Dunick, Walter T. (CMS/OIS); Lazenby, Daniel (CMS/OIS); polise_anthony@bah.com; Paul.Donohoe@cms.hhs.gov; Lewis, Angela [USA] (Lewis_Angela@bah.com); Grace.Suk@cms.hhs.gov; [redacted] (CGI Federal); [redacted] (CGI Federal); Mohs, Dean F. (CMS/CCIIO); Schneer, Seth H. (CMS/CCIIO); Grace.Suk@cms.hhs.gov; Luan Nguyen (luan.nguyen@relis-llc.com); [redacted] (CGI Federal); Amos, Robert E. (CMS/OC) (Robert.Amos@cms.hhs.gov); Duve, Rebecca J. (CMS/CTR) (Rebecca.Duve@cms.hhs.gov); 'Hase, Jason' (Jason.Hase@noblis.org); Rowen, Stanley [USA]; Hoang, Teresa [USA]; colin.mcveigh@cms.hhs.gov; [redacted] (CGI Federal); Couts, Todd (CMS/OIS) (Todd.Couts1@cms.hhs.gov) (Todd.Couts1@cms.hhs.gov); [redacted] (CGI Federal); [redacted] CGI Federal)
Subject: RE: Updated FFM Integrated Schedule
Attachments: FFM_IMS.zip

Hi Tyrone,

Please find the updated FFM Schedule as of Aug 17th in the attachment. We had a major review on all the tasks and the % completes for all the pages and services are all revised and updated. Please let me know if I can provide more information. Thank you!

Name	% Complete
FFM	55%
Eligibility and Enrollment	61%
Financial Management	14%
Plan Management	80%
Technical Architecture	69%
Infrastructure and Operational Readiness	51%

Contains Sensitive and Proprietary Business Information -- Maintain as Confidential

Exhibit 23

CGI. Email between Monica Winthrop and CMS officials. IMPLIA Status at 12:31 AM on 9/24.
Sept. 24, 2013.

From: [redacted] (CGI Federal) [redacted]]
Sent: Tuesday, September 24, 2013 12:48 AM
To: Outerbridge, Monique (CMS/OIS (monique.outerbridge@cms.hhs.gov); Oh, Mark U. (CMS/OIS) (mark.oh@cms.hhs.gov); Miller, Daniel J. (CMS/OIS) (daniel.miller2@cms.hhs.gov); Van, Hung B. (CMS/OIS) (Hung.Van@cms.hhs.gov); Chao, Henry (CMS/OIS) (henry.chao@cms.hhs.gov) (henry.chao@cms.hhs.gov); Robert.Thurston@cms.hhs.gov; Um, Peter (CMS/CTR) (Peter.Um1@cms.hhs.gov); Walter, Stephen J. (CMS/OIS) (stephen.walter@cms.hhs.gov)
CC: [redacted] (CGI Federal); [redacted] (CGI Federal); [redacted] (CGI Federal)
Subject: IMPL1A Status at 12:31AM on 9/24

CGI was able to successfully execute all 6 scenarios that are given to issuers to test the FFM online application. During the course of testing we identified two issues:

- A time out setting in Akamai was causing time out errors in some application scenarios. Once the Akamai settings were increased, the time out error condition stopped when we ran through the six scenarios.

- Additionally, we found that under certain scenarios involving custom groups (not selecting the default), an infinite loop was spawned that degraded server performance. We were able locate the problem code. A fix is being worked and we expect we will be able to apply a hot fix sometime tomorrow. In the meantime, we will monitor server performance and alert you if we see any server degradation.

Below is a summary of the six scenarios we tested with (these are the same the issuers are using):

Test Case #	State/Zip Code	Dental Plan Enrolled	Health Plan Enrolled	Notes
TC834001	ID/83403	Passed	Passed	Scenario has too much income to get APTC
TC834002	AK/72002	Passed	Passed	
TC834003	VA/22206	Passed	Passed	
TC834004	ID/83403	Passed	Passed	Scenario has too much income to get APTC
TC834005	IL/61265	Passed	Passed	EHB amount $0 for zip code, therefore no APTC reduced from plan
TC834006	AZ/85008	Passed	Passed	

We are encountering the following known issues, which either have no impact or there are simple work arounds:

Contains Sensitive and Proprietary Business Information -- Maintain as Confidential

- After successfully account creation login fails with downstream error (workaround – close browser and log back in with newly created account)
- Undefined Error message on account verification (no impact)
- No confirmation on Address verification (no impact)
- View Eligibility Results from My Account (workaround – get Eligibility Results from Eligibility Results screen in Individual Application)
- When creating a new account – received an undefined error on ID proofing page (although it was verified).

  Second attempt – created an account successfully but getting a downstream error when logging in using the same.

- Groupings should not be changed in Plan Compare, this is causing a utility on the server to loop and increase the memory usage.

Each of these issues is assigned to a technical resource for resolution.

Also, the APTC issue due to missing EHB data for dental plans has been resolved through a data load which was verified tonight. We will move that to Prod once CMS gives the ok.

Please let me know if you have any questions.

Thanks,

[redacted]

[redacted] PMP | Director, Consulting | CGI Federal | [redacted] | [redacted] |
[redacted]

CONFIDENTIALITY NOTICE: Proprietary/Confidential Information belonging to CGI Group Inc. and its affiliates may be contained in this message. If you are not a recipient indicated or intended in this message (or responsible for delivery of this message to such person), or you think for any reason that this message may have been addressed to you in error, you may not use or copy

Contains Sensitive and Proprietary Business Information -- Maintain as Confidential

CGISEN100026760

or deliver this message to anyone else. In such case, you should destroy this message and are asked to notify the sender by reply e-mail.

Contains Sensitive and Proprietary Business Information -- Maintain as Confidential

CGISEN100026761

Exhibit 24

Emails between CGI and CMS officials concerning outstanding issues. Sept. 29, 2013.

(CMS/OIS); Couts, Todd (CMS/OIS); Thompson, Tyrone (CMS/OIS)
Subject: Re: Status of OIS and Issuer Priority Defects

Good morning, Monique. The ones in testing are in the test region and are being tested.

Thanks,

Justin

Please excuse typos - this email was sent from my iPhone

On Sep 29, 2013, at 7:25 AM, "Outerbridge, Monique (CMS/OIS)" <monique.outerbridge@cms.hhs.gov> wrote:

By the way, the ones in testing are in what test region or are you saying you're currently unit testing them?

From: [redacted] (CGI Federal) [redacted]
Sent: Sunday, September 29, 2013 1:43 AM
To: Outerbridge, Monique (CMS/OIS); [redacted] (CMS/OIS); [redacted] (CGI Federal); [redacted] (CMS/CTR); [redacted] (CMS/CPI); [redacted] (CMS/OIS); [redacted] (CMS/CTR); Oh, Mark U. (CMS/OIS)
Cc: [redacted]CGI Federal); [redacted] (CGI Federal); Chao, Henry (CMS/OIS); [redacted] (CMS/OIS); Couts, Todd (CMS/OIS); Thompson, Tyrone (CMS/OIS)
Subject: RE: Status of OIS and Issuer Priority Defects

Monique,

Per your request, below is the list of outstanding issues. Many are still in testing and I will provide a status in the morning. I have also mapped them to your presentation for your report back out.

Please let me know if you have any questions.

Thanks,

Monica

Contains Sensitive and Proprietary Business Information -- Maintain as Confidential

Day 1 Experience Description	Description
Consumer: Obtain Eligibility Determination	Date/Time stamp is not stored consistently through the application
Consumer: Obtain Eligibility Determination	Full Medicaid language on Eligibility Results
Consumer: Create an Account	Trying to create a new application when saving and returning is treating as a ne
Consumer: Obtain Eligibility Determination	CSR not picking up annual income amount
Consumer: Notices	Completion of Eligibility Notices
Consumer: Obtain Eligibility Determination	The text informing the applicant they are a multi-tax household that must "wai appears on the screen; this does not affect the actual enrollment
Consumer: Obtain Eligibility Determination	ESC MEC is not writing the indicator to the event. So APTC sees default as No a
Consumer: Obtain Eligibility Determination	MAGI 3: Modify the deprived child rule: parent hours worked should look for th not on the parent.
Consumer: Obtain Eligibility Determination	MAGI 3: Debug/fix CHIP waiting period rule. Is not finding people ineligible unc period. 94506, VA
Consumer: Obtain Eligibility Determination	Residency: Not setting residency Pend for Medicaid when applicant is tempora out of state
Consumer: Obtain Eligibility Determination	Residency: Parent child apply for coverage, parent in state in which applying; ch eligible for qhp/aptc. Child is not. 90325, IN. DE014
Consumer: Compare Plans and Select Plan for Enrollment	Effective Date 12/31 instead of 1/1
Consumer: Obtain Eligibility Determination	Non-ESI MEC: Not seeing events for the Non-ESI MEC call from DIE
Issuer: Enrollment Transactions	Missing Race/Ethnicity on 834
Consumer: Compare Plans and Select Plan for Enrollment	Pay Redirect SAML assertions
Consumer: Apply for Insurance	Agent / Broker
Consumer: Compare Plans and Select Plan for Enrollment	Unable to enroll all children when the share the same DOB (e.g. twins, triplets)
Eligiblity Support Worker	ESD: Unable to view notices
Consumer: Apply for Insurance	Not saving all attestations

Thanks,

Monica

Monica Winthrop, PMP | Director, Consulting | CGI Federal | O: 703-227-6012 | C: 571-533-9389 | monica.winthrop@cgifederal.com

CONFIDENTIALITY NOTICE: Proprietary/Confidential Information belonging to CGI Group Inc. and its affiliates may be contained in this message. If you are not a recipient indicated or intended in this message (or responsible for delivery of this message to such person), or you think for any reason that this message may have been addressed to you in error, you may not use or copy or deliver this message to anyone else. In such case, you should destroy this message and are asked to notify the sender by reply e-mail.

From: Outerbridge, Monique (CMS/OIS) [mailto:monique.outerbridge@cms.hhs.gov]
Sent: Saturday, September 28, 2013 7:13 PM
To: Winthrop, Monica (CGI Federal); Van, Hung B. (CMS/OIS); Ponnada, Ramesh (CGI Federal);

Contains Sensitive and Proprietary Business Information -- Maintain as Confidential

Exhibit 25

CMS. Health Insurance Marketplace Update. Test Summary Report. Learn/Help Center/Sprints 1.5 & 1.6. Undated. Prepared by Aquilent.

DEPARTMENT OF HEALTH & HUMAN SERVICES
Centers for Medicare & Medicaid Services
7500 Security Boulevard, Mail Stop 00-00-00
Baltimore, Maryland 21244-1850

Office of Communications

Health Insurance Marketplace Update

Test Summary Report

Learn/Help Center/Sprints 1.5 & 1.6

Contents

Health Insurance Marketplace Update 1
Test Summary Report 1
1 INTRODUCTION 2
1.1 PURPOSE 2
1.2 SCOPE 2
1.3 TESTING ANALYSIS 2
1.4 DOCUMENT REFERENCES 3
2 TESTING 4
2.1 PASS/FAIL CRITERIA 4
2.1.1 Pass 4
2.1.2 Fail 4
2.1.3 Blocked 4

1 INTRODUCTION

Testing for the October 1, 2013 release of the Health Insurance Marketplace update project was completed on September 30th, 2013. Following the testing, the development team worked in the Akamai development environment to resolve reported issues according to priority. The summary results of functional integration testing for this phase of the HIM project are documented in this report.

1.1 PURPOSE

This Test Summary Report (TSR) summarizes the results of testing for the HIM October 1, 2013 release only. Functional testing encompasses all system and regression testing. Functional testing consisted of inspection Testing, Front End Functionality, and Back End Functionality, cross browser, and Section 508 verification. Basic integration testing between the Learn and Marketplace sites was conducted.

1.2 SCOPE

The scope for testing was represented by 63 test cases. Initial testing verified compliance to documented requirements. Confirmation testing verified defect fixes, code and configuration changes, and any other changes to the test2 environment, test data, test cases, or project documentation made in response to defects reported during testing. This TSR contains the analysis of all functional testing performed by the Aquilent test team.

All testing was conducted on test2. Integration testing was attempted on test2, prodprime, and imp1a with limited success. Testers were, at times, unable to complete integration between the Gateway and the Marketplace when using Firefox and IE10. Testers were also unable to verify session timeout so this logic was removed from the Learn site just prior to the site launch.

1.3 TESTING ANALYSIS

During testing 113 issues were logged (September 10-October 5). Of those issues, 106 were determined to be defects. Four were duplicates, two could not be reproduced and were closed, and one was set to Won't Fix. These defects were processed through the documented defect resolution workflow (see Section 3).

Table 1: Defects Logged

Severity Level	Count
Blocker	6
Critical	20
Major	55

Severity Level	Count
Minor	17
Trivial	8
TOTAL	**106**

Of the 106 valid defects logged, 51 were resolved and validated. Currently, there are 55 unresolved defects, 2 of which are Blockers, 2 of Critical severity, 30 Major, 14 Minor, and 7 Trivial. All defects logged for this release can be found at this link.

Of the 63 test cases executed for this release, 40 passed and 23 failed. Specifics related to individual successes and failures for each test case can be found in the October 1 Test Cycle under HC2-Learn or at this link.

1.4 **DOCUMENT REFERENCES**

The information used in preparing this document was taken directly from the Jira database used to record, track, and resolve defects and in tracking test case progress. Links to defects or test cases can be found in section 1.3.

2 TESTING

Tests cases were executed using the October 1 Release test cycle in JIRA under the HC2 Learn project. Each test in the cycle is marked as Passed or Failed and any tickets associated to the test execution are noted in the Defect column. Any details specific to a failed test step are contained within each test case on the applicable step level.

2.1 PASS/FAIL CRITERIA

The test case execution workflow is managed by assigning a status to all test cases. All test cases start with the status of Unexecuted. During the test execution cycle, all in-scope tests are executed. As tests are completed, the test case moves to In progress, the to Pass, Fail, or Blocked, depending on the outcome.

2.1.1 Pass

Test cases are considered Passed when:

- Actual results match test case expected results.
- When actual results do not match expected results, a defect is logged in Jira. If the defect is set to As Designed, won't fix, or cannot reproduce status, a variance has been accepted and is the test is considered to be passed.

2.1.2 Fail

Test cases are considered Failed when:

- Actual results do not match expected results and the defect is accepted by the development team.

2.1.3 Blocked

Test cases are considered Blocked when the test cannot be fully executed due to a problem that is not directly related to the test case. Blocked test cases are usually the result of some dependency not being satisfied – usually related to code or environment issues. Tests with a Blocked status may be fully or only partially blocked.