

Department of Health & Human Services  
Centers for Medicare & Medicaid Services  
7500 Security Boulevard, Mail Stop N2-20-16  
Baltimore, Maryland 21244-1850



Office of Strategic Operation and Regulatory Affairs/Freedom of Information Group  
Refer to Control Number: 122020137058

---

May 15, 2015

Mr. William F. Marshall  
Judicial Watch  
425 Third Street, S.W.  
Suite 800  
Washington, D.C. 20024

Dear Mr. Marshall:

This is the fifth interim response to your December 20, 2013 Freedom of Information Act (FOIA) request addressed to the CMS FOIA Officer, Centers for Medicare & Medicaid Services (CMS), Freedom of Information Group. Your request sought access to the following records:

Any and all records related to, regarding or in connection with the security of healthcare.gov web portal including, but not limited to, studies, memoranda, correspondence, electronic communications (emails), and slide presentations from January 1, 2012 to the present date.

On June 13, 2014, you modified the scope of your FOIA request to exclude records consisting of lines of computer code and records that would otherwise leave the healthcare.gov website vulnerable to attack if released to the public. You emphasized that this modification covers technical documents only, and that HHS records merely stating or generally discussing the existence of a potential problem with the website were still within the parameters of your request.

In this interim response we have processed a total of 884 pages. Two hundred forty-four (244) pages are released in their entirety, three hundred seventy-one (371) pages are released in part, and two hundred fifty-nine (259) pages are withheld in full. All of these pages are enclosed and have been bates numbered. Ten (10) pages have been intentionally blank.

Comprised within the 630 pages redacted either in full or in part is material that is either: 1. Within the scope of the June 13, 2014 modification of your request, and therefore considered non-responsive to your request; 2. Exempt from disclosure pursuant to the deliberative process privilege of Exemption 5, or 3. Exempt from disclosure pursuant to Exemption 6.<sup>1</sup>

---

<sup>1</sup> Please note with respect document number CMS00000003\_00000005, attachments to this record include document numbers CMS00000003\_00000006 – 14. Although document numbers CMS000003\_000006, 7, 9 and 11 were produced with the 4th Interim Response letter, bates #s CMS000528-541, we are re-releasing these records for your convenience, along with attachments CMS00000003\_00000008, 10, 12-14. With respect document number CMS00000003\_00025405, attachments to this record include links to databases that were not copied and are not accessible for production.

Mr. William F. Marshall  
May 15, 2015  
Page Two

Exemption b(5), Deliberative Process Privilege: FOIA Exemption 5 permits a federal agency to withhold inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with an agency.

Exemption 6: FOIA Exemption 6 permits a federal agency to withhold information about individuals in "personnel and medical files and similar files" when the disclosure of such information "would constitute a clearly unwarranted invasion of personal privacy."

Please be advised that CMS's review of records located which may be responsive to your modified request remains active and ongoing. As additional responsive records are reviewed, CMS will promptly release all non-exempt records that are responsive to your request.

Sincerely yours,

Hugh P. Gilmore -S

Digitally signed by Hugh P. Gilmore -S  
DN: c=US, o=U.S. Government, ou=HHS, ou=CMS, ou=People,  
0.9.2342.19200300.100.1.1=2001527759, cn=Hugh P. Gilmore -  
S  
Date: 2015.05.15 10:55:00 -04'00'

Hugh Gilmore  
Director  
Freedom of Information Group

Enclosure (884pages)

Appointment

**From:** Margush, Doug C. [NotResp]  
 [NotResp]  
**Sent:** 10/1/2013 12:39:07 AM  
**To:** Margush, Doug C. (CMS/OIS) [NotResp]  
 [NotResp] Booth, Jon G. (CMS/O [NotResp]  
 [NotResp] Chao, Henry (CMS/OIS) [NotResp]  
 [NotResp] Mike Finkel (mfinkel@qssinc.com) [mfinkel@qssinc.com];  
 Walter, Stephen J. (CMS/OIS) [NotResp]  
 [NotResp] Karlton Kim (kkim@qssinc.com) [kkim@qssinc.com];  
 Sharma, Hemant (CGI Federal) (Hemant.Sharma@cgifederal.com) [Hemant.Sharma@cgifederal.com]; Oh, Mark U.  
 (CMS/OIS) [NotResp]  
 [NotResp] Um, Peter (CMS/CTR) [NotResp]  
 [NotResp] Thurston,  
 Robert (CMS/CTR) [NotResp] Keith  
 Rubin [Keith.Rubin@cgifederal.com]; Schankweiler, Thomas W. (CMS/OIS) [NotResp]  
 [NotResp] Richardson, Marc D. (CMS/OIS) [NotResp]  
 [NotResp] Basavaraju, Venkat  
 (CMS/OIS) [NotResp] Linares, George  
 E. (CMS/OIS) [NotResp]  
 Stevenson, Corey B. (CMS/OIS) [NotResp]  
 [NotResp] Gray, Edward M. (CMS/OIS) [NotResp]  
 [NotResp] Berkley, Katrina (CMS/OIS) [NotResp]  
 [NotResp] Van, Hung B. (CMS/OIS)  
 [NotResp]  
 O'Kussick, James J. (CMS/OIS) [NotResp]  
 Skinner, Dennis R. (CMS/OIS) [NotResp]  
 [NotResp] Grothe, Kirk A. (CMS/OIS) [NotResp]  
 [NotResp] Driscoll, Adam (CMS/OIS)  
 [NotResp] Fender, Rebecca (CMS/CCSQ)  
 [NotResp] Patel, Ketan (CMS/OC)  
 [NotResp] Carter, Daniel (CMS/OC)  
 [NotResp]  
**CC:** Orlando, Mark (CMS/CTR) [NotResp]  
 [NotResp] Villar, Manuel  
 (mvillar@CCSIN.COM) [mvillar@CCSIN.COM]; Perry Patterson [NotResp]  
 [NotResp]

**Subject:** FW: Early warning strategy to guard overload conditions in EIDM, FFM, and Hub

**Location:** (b)(6)

**Start:** 10/1/2013 1:15:00 AM

**End:** 10/1/2013 2:15:00 AM

**Show Time As:** Tentative

**Importance:** High

**Recurrence:** (none)

-----Original Appointment-----

**From:** Margush, Doug C. (CMS/OIS)

**Sent:** Monday, September 30, 2013 3:52 PM

**To:** Margush, Doug C. (CMS/OIS); Chao, Henry (CMS/OIS); Mike Finkel ([mfinkel@gssinc.com](mailto:mfinkel@gssinc.com)); Walter, Stephen J. (CMS/OIS); Karlton Kim ([kkim@gssinc.com](mailto:kkim@gssinc.com)); Sharma, Hemant (CGI Federal) ([Hemant.Sharma@cgifederal.com](mailto:Hemant.Sharma@cgifederal.com)); Oh, Mark U. (CMS/OIS); Um, Peter (CMS/CTR); Thurston, Robert (CMS/CTR); Keith Rubin; Schankweiler, Thomas W. (CMS/OIS); Richardson, Marc D. (CMS/OIS); Basavaraju, Venkat (CMS/OIS); Linares, George E. (CMS/OIS); Stevenson, Corey B. (CMS/OIS); Gray, Edward M. (CMS/OIS); Berkley, Katrina (CMS/OIS); Van, Hung B. (CMS/OIS); O'Kussick, James J. (CMS/OIS); Skinner, Dennis R. (CMS/OIS); Grothe, Kirk A. (CMS/OIS); Driscoll, Adam (CMS/OIS); Fender, Rebecca (CMS/CCSQ); Patel, Ketan (CMS/OC); Carter, Daniel (CMS/OC)

**Cc:** Orlando, Mark (CMS/CTR); 'Villar,Manuel ([mvillar@CCSIN.COM](mailto:mvillar@CCSIN.COM))'; Perry Patterson

**Subject:** Early warning strategy to guard overload conditions in EIDM, FFM, and Hub

**When:** Monday, September 30, 2013 9:15 PM-10:15 PM (UTC-05:00) Eastern Time (US & Canada).

**Where:** (b)(6)

**Importance:** High

Rescheduled. Ketan, know your Akamai stuff should be starting around this time.

---

**From:** Chao, Henry (CMS/OIS)

**Sent:** Monday, September 30, 2013 3:35 PM

**To:** Mike Finkel ([mfinkel@gssinc.com](mailto:mfinkel@gssinc.com)); Walter, Stephen J. (CMS/OIS); Karlton Kim ([kkim@gssinc.com](mailto:kkim@gssinc.com)); Sharma, Hemant (CGI Federal) ([Hemant.Sharma@cgifederal.com](mailto:Hemant.Sharma@cgifederal.com)); Oh, Mark U. (CMS/OIS); Um, Peter (CMS/CTR); Thurston, Robert (CMS/CTR); Keith Rubin; Margush, Doug C. (CMS/OIS); Schankweiler, Thomas W. (CMS/OIS); Richardson, Marc D. (CMS/OIS); Basavaraju, Venkat (CMS/OIS); Linares, George E. (CMS/OIS); Stevenson, Corey B. (CMS/OIS); Gray, Edward M. (CMS/OIS); Berkley, Katrina (CMS/OIS); Van, Hung B. (CMS/OIS)

**Cc:** George Schindler ([george.schindler@cgi.com](mailto:george.schindler@cgi.com)); 'Cheryl.Campbell@cgifederal.com'; Rich Martin ([Rich.Martin@cgifederal.com](mailto:Rich.Martin@cgifederal.com)); Bikram Bakshi ([bbakshi@gssinc.com](mailto:bbakshi@gssinc.com)); Outerbridge, Monique (CMS/OIS); Grothe, Kirk A. (CMS/OIS); Nelson, David J. (CMS/OEM); Skinner, Dennis R. (CMS/OIS); Royle, Erick B. (CMS/OIS); Shahegh, Yousef (CMS/OIS); Coutts, Todd (CMS/OIS); Berkley, Katrina (CMS/OIS); Rhones, Rhonda D. (CMS/OIS); O'Kussick, James J. (CMS/OIS); Roche, Jacqueline R. (CMS/CCIIO); Fender, Rebecca (CMS/CCSQ); Driscoll, Adam (CMS/OIS)

**Subject:** Early warning strategy to guard overload conditions in EIDM, FFM, and Hub

**Importance:** High

Sometime later today we need to convene a meeting to discuss how we will set monitoring tools (yours/mine/ours) and their configurations, alerts types and categories, who/whom gets alerted, actions following an alert, response procedures, communication (internal across CMS and contractor and external to partners and consumers), and exit/close-out rules.

The primary objective is to monitor and detect early when a part or parts of the network, infrastructure, and systems begin to show sign of issues related to overload of users, requests, queues, wait times, timeouts, etc. and we initiate based on agreed upon roles and responsibilities (along with the internal and external messaging) to throttle the degrading situation with performance and capacity.

For example if EIDM is seeing 25,000 new registrants every hour and the capacity was designed to only handle 20,000 New registrations in an hour then some monitoring configuration and trigger should be set to either a threshold of 15,000 in increments to 20,000 and/or detection of long running processes stuck in infinite loops or too many hung in a



state. Either or both will create a poor experience for the user (consumers, Agents and Brokers, Navigators, Assistants, Issuers, CCRs, Employers, Employees, ESW, states, etc.). so at the early warning we would take action to either post a message on the top level HC.gov quickly and send an alert to all the call centers and help desks (in addition to the system admins) to invoke procedures to help throttle traffic and even perform a temporary shutdown rather than letting the system go out of control and then makes it next to impossible to recover what was in stream at the time it crashed.

So the following are some high level example areas we need to agree on for monitoring and setting configs and thresholds so you can start working on before we even come together:

Fed agency response times and SLAs

Hub SLAs with Fed agencies, Issuers, and FFM

Verification services (by each verification source, routing, valid requests and responses, etc.)

RIDP response times, help desk workloads and progress, exceeding threshold for failures (e.g., >30%)

EIDM New Registration

EIDM log in

Portal status

Portlet status

CMSNet status

Healthcare.gov (learn, get insured, and Spanish)

General application performance for consumers anywhere in the application

Specific points in the application such as Plan Compare

Notice generation

834 generation

EFT services

Internet status (at BDC and at TMRK)

Security events

...

Doug, hung, and Steve—can you coordinate and gather the folks to the meeting later today to get their answers and plans documented.

Thanks

Henry Chao

Deputy CIO & Deputy Director,

Office of Information Services

Centers for Medicare & Medicaid Services

410-786-1800

Appointment

From:	Couts, Todd (CMS/OIS)	NotResp	
	NotResp		
Sent:	9/30/2013 3:10:43 PM		
To:	Couts, Todd (CMS/OIS)	NotResp	
	NotResp	Grothe, Kirk A. (CMS/OIS)	NotResp
	NotResp		
	Outerbridge, Monique (CMS/OIS)	NotResp	
	NotResp	Cole, Reba R. (CMS/OIS)	NotResp
	NotResp	Keates, Nancy J. (CMS/OIS)	NotResp
	NotResp		Oh, Mark
	U. (CMS/OIS)	NotResp	
	NotResp	; Van, Hung B. (CMS/OIS)	NotResp
	NotResp		Radcliffe, Glenn D. (CMS/OIS)
	NotResp		
	Simons, Kingsley L. (CMS/OIS)	NotResp	
	NotResp	Booth, Jon G. (CMS/OC)	NotResp
	NotResp	Patel, Ketan (CMS/OC)	NotResp
	NotResp	Skinner, Dennis R. (CMS/OIS)	NotResp
	NotResp		Royle, Erick B. (CMS/OIS)
	NotResp		Margush, Doug C.
	(CMS/OIS)	NotResp	Chao,
	Henry (CMS/OIS)	NotResp	Alvarez, Carlos
	(CMS/OIS)	NotResp	
	NotResp	Birkmire, Tom (CMS/OIS)	NotResp
	NotResp		
	NotResp		Dunick, Walter T. (CMS/OIS)
	NotResp		Schankweiler, Thomas
	W. (CMS/OIS)	NotResp	Lyles,
	Darrin V. (CMS/OIS)	NotResp	
	NotResp	Burke, Sheila M. (CMS/OIS)	NotResp
	NotResp	Bush-Warren, Theresa (CMS/OIS)	NotResp
	NotResp		
	NotResp	Nebolsine, Samantha L. (CMS/OIS)	NotResp
	NotResp		
	NotResp	Bell, Amber J. (CMS/OL)	NotResp
	NotResp		Lelis,
	Nikoleta (CMS/OIS)	NotResp	
	NotResp	Leong, Kelly (CMS/OIS)	NotResp
	NotResp	Speights, Richard A. (CMS/OIS)	NotResp
	NotResp		
	Lazenby, Daniel (CMS/OIS)	NotResp	
	NotResp	; Donohoe, Paul X. (CMS/OIS)	NotResp
	NotResp	Gray, Brian (CMS/OIS)	NotResp
	NotResp		
	NotResp		Ross, Cassandra (CMS/OIS)
	NotResp		NotResp
	NotResp		
	Holden, Stacey (CMS/OIS)	NotResp	
	NotResp	Trudel, Karen	NotResp
	NotResp	Richardson, Marc D. (CMS/OIS)	NotResp
	NotResp		
	Basavaraju, Venkat (CMS/OIS)	NotResp	

NotResp

James, Brian M. (CMS/CCIO)

NotResp

NotResp

Underwood, Damon L. (CMS/OIS)

NotResp

NotResp

'Piazza\_Tara@bah.com' (Piazza\_Tara@bah.com) [Piazza\_Tara@bah.com]; Rich Martin (Rich.Martin@cgifederal.com) [Rich.Martin@cgifederal.com]; cheryl.campbell@cgifederal.com; george.schindler@cgi.com; Karlton Kim (kkim@qssinc.com) [kkim@qssinc.com]; 'Jagadish Gangahanumaiah' (jgangahanumaiah@qssinc.com) [jgangahanumaiah@qssinc.com]; Fred Covert - US (fcovert@caci.com) [fcovert@caci.com]; Par Rachakonda - US (prachakonda@caci.com) [prachakonda@caci.com]; rich.schwarzkopf (rich.schwarzkopf@urs.com) [rich.schwarzkopf@urs.com]; Geraldine Clawson (gclawson@verizon.com) [gclawson@verizon.com]; Deepak Bhatta (dbhatta@qssinc.com) (dbhatta@qssinc.com) [dbhatta@qssinc.com]; 'Nick Mistry (Nick.Mistry@eglobaltech.com) (Nick.Mistry@eglobaltech.com)' [Nick.Mistry@eglobaltech.com]; Dave Merrill (Dave.Merrill@eglobaltech.com) [Dave.Merrill@eglobaltech.com]; Thurston, Robert (CMS/CTR)

NotResp

NotResp

Um, Peter (CMS/CTR)

NotResp

NotResp

Fletcher, John

A.

NotResp

Feuerberg, Lisa A. (CMS/OIS)

NotResp

Adkins, Laura J. (CMS/OIS)

NotResp

NotResp

Thompson, Tyrone (CMS/OIS)

NotResp

NotResp

; Mike

Finkel (mfinkel@qssinc.com) [mfinkel@qssinc.com]; Rhones, Rhonda D. (CMS/OIS)

NotResp

NotResp

Berkley,

Katrina (CMS/OIS)

NotResp

Miller, Daniel J. (CMS/OIS)

NotResp

Tran,

Thy N. (CMS/OIS)

NotResp

NotResp

Fender, Rebecca (CMS/CCSQ)

NotResp

NotResp

'monica.winthrop@cgifederal.com'

[monica.winthrop@cgifederal.com]; 'Leak, Jennifer J (CGI Federal)' (Jennifer.Leak@cgifederal.com)

[Jennifer.Leak@cgifederal.com]; Schmidt, Donna W. (CMS/OIS)

NotResp

NotResp

Johnston, James (CMS/CMMI)

NotResp

NotResp

Bowen, Victoria F (CGI Federal) [victoria.bowen@cgifederal.com]; Ling, Candice (CGI Federal)

[Candice.Ling@cgifederal.com]; Carter, Brandi (CGI Federal) (Brandi.Carter@cgifederal.com)

(Brandi.Carter@cgifederal.com) [Brandi.Carter@cgifederal.com]

CC:

'Kingswell, Brett [USA]' [kingswell\_brett@bah.com]; 'Kannan, Nari [USA]' [Kannan\_Nari@bah.com]; Wongus, Alethia

C. (CMS/OIS)

NotResp

Purcell,

Timothy J. (CMS/OIS)

NotResp

Chao,

Bing (CMS/OIS)

NotResp

NotResp

Subject: MEETING: IT CCB Kickoff

Location: (b)(6) // XOC Conference Room // Bethesda Paris Room

Start: 10/2/2013 2:30:00 PM

End: 10/2/2013 3:30:00 PM

Show Time As: Busy

Recurrence: (none)

**Required Attendees:** Grothe, Kirk A. (CMS/OIS); Outerbridge, Monique (CMS/OIS); Cole, Reba R. (CMS/OIS); Keates, Nancy J. (CMS/OIS); Oh, Mark U. (CMS/OIS); Van, Hung B. (CMS/OIS); Radcliffe, Glenn D. (CMS/OIS); Simons, Kingsley L. (CMS/OIS); Booth, Jon G. (CMS/OC); Patel, Ketan (CMS/OC); Skinner, Dennis R. (CMS/OIS); Royle, Erick B. (CMS/OIS); Margush,

Doug C. (CMS/OIS); Chao, Henry (CMS/OIS); Alvarez, Carlos (CMS/OIS); Birkmire, Tom (CMS/OIS); Dunick, Walter T. (CMS/OIS); Schankweiler, Thomas W. (CMS/OIS); Lyles, Darrin V. (CMS/OIS); Burke, Sheila M. (CMS/OIS); Bush-Warren, Theresa (CMS/OIS); Nebolsine, Samantha L. (CMS/OIS); Bell, Amber J. (CMS/OL); Lelis, Nikoleta (CMS/OIS); Leong, Kelly (CMS/OIS); Speights, Richard A. (CMS/OIS); Lazenby, Daniel (CMS/OIS); Donohoe, Paul X. (CMS/OIS); Gray, Brian (CMS/OIS); Ross, Cassandra (CMS/OIS); Holden, Stacey (CMS/OIS); Trudel, Karen (CMS/OIS); Richardson, Marc D. (CMS/OIS); Basavaraju, Venkat (CMS/OIS); James, Brian M. (CMS/CCIO); Underwood, Damon L. (CMS/OIS); 'Piazza\_Tara@bah.com' (Piazza\_Tara@bah.com); 'Rich Martin (Rich.Martin@cgifederal.com)'; 'cheryl.campbell@cgifederal.com'; 'george.schindler@cgi.com'; 'Karlton Kim (kkim@qssinc.com)'; 'Jagadish Gangahanumaiah' (jgangahanumaiah@qssinc.com); 'Fred Covert - US (fcovert@caci.com)'; 'Par Rachakonda - US (prachakonda@caci.com)'; 'rich.schwarzkopf (rich.schwarzkopf@urs.com)'; 'Geraldine Clawson (gclawson@verizon.com)'; 'Deepak Bhatta (dbhatta@qssinc.com) (dbhatta@qssinc.com)'; 'Nick Mistry (Nick.Mistry@eglobaltech.com) (Nick.Mistry@eglobaltech.com)'; 'Dave Merrill (Dave.Merrill@eglobaltech.com)'; Thurston, Robert (CMS/CTR); Um, Peter (CMS/CTR); Fletcher, John A. (CMS/OIS); Feuerberg, Lisa A. (CMS/OIS); Adkins, Laura J. (CMS/OIS); Thompson, Tyrone (CMS/OIS); 'Mike Finkel (mfinkel@qssinc.com)'; Rhones, Rhonda D. (CMS/OIS); Berkley, Katrina (CMS/OIS); Miller, Daniel J. (CMS/OIS); Tran, Thy N. (CMS/OIS); Fender, Rebecca (CMS/CCSQ); 'monica.winthrop@cgifederal.com'; 'Leak, Jennifer J (CGI Federal)' (Jennifer.Leak@cgifederal.com); Schmidt, Donna W. (CMS/OIS); Johnston, James (CMS/CMMI); Bowen, Victoria F (CGI Federal); Ling, Candice (CGI Federal); Carter, Brandi (CGI Federal) (Brandi.Carter@cgifederal.com) (Brandi.Carter@cgifederal.com)

**REMINDER:** Meeting is still on

- Logistics:

(b)(6)

- XOC Conference Room
- Bethesda Paris Room
- Slides coming soon

All,

Please hold this time for a kickoff of the IT CCB. With our Go-Live, we need to kickoff and restart change control procedures for a full production environment. Starting tomorrow (10/1), we want to run all infrastructure and application changes through this process and board. Please make every effort to attend as it was impossible to find a free time on everyone's calendar.

Also, please note a few key things:

- Below, please find the membership and voting members. Please send any tweaks you might have.
- Through October and November, we will setup IT CCB meetings twice per week (Tuesdays and Thursdays). After that, we can hopefully go to once per week.

## Membership List for the IT CCB

### OIS Representatives

Role	Name	
CCB Co-Chair	Kirk Grothe	
CCB Co-Chair	Todd Coutts	
Change Coordinator	Primary: Reba Cole Backup: Nancy Keates	
FFM and Hub Technical Lead	Primary: Mark Oh Backup: Hung Van	Voting Member
MIDAS Technical Lead	Primary: Glenn Radcliffe Backup: Kingsley Simons	Voting Member
Healthcare.gov	Primary: Jon Booth Backup: Ketan Patel	Voting Member
Operations	Primary: Dennis Skinner Backup: Erick Royle	Voting Member
Infrastructure	Primary: Doug Margush Backup: TBD	Voting Member
E&E IT Project Manager	Primary: Hung Van Backup: Bing Chao	Voting Member
Plan Management IT Project Manger	Primary: Carlos Alvarez Backup: Tom Birkmire	Voting Member
Financial Management IT Project Manager	Primary: Walt Dunick Backup: TBD	Voting Member
Security Operations	Primary: Thomas Schankweiler Backup: Darrin Lyles	Voting Member
Help Desk	Primary: Sheila Burke Backup: Theresa Bush-Warren	Subject Matter Expert
Issuer Operations Team	Primary: Samantha Nebolsine Backup: Amber Bell	Subject Matter Expert
State Operations	Primary: Nikoleta Lewis Backup: Kelly Leong	Subject Matter Expert
Federal Operations	Primary: Richard Speights Backup: Daniel Lazenby	Subject Matter Expert



Testing Team	Primary: Paul Donohoe Backup: TBD	Subject Matter Expert
Triage Team	Primary: Brian Gray Backup: Cassandra Ross	Subject Matter Expert
Release Management & CI/CID	Stacey Holden & Cassandra Ross	Subject Matter Expert
Shared Services (EIDM and Portal)	Karen Trudel, Marc Richardson, Venkat Basavaraju	Subject Matter Expert
HIOS	Brian James	Subject Matter Expert
OIS CALT Coordinator	Damon Underwood	CCB Support
OIS CALT Coordinator-Backup	Cassandra Ross	CCB Support
CCB Contractual Support Lead	Tara Piazza (Booz Allen)	CCB Support

#### IT Contractor Representatives

Role	Contractor	Name
FFM System	CGI	
Data Services Hub	QSSI	
MIDAS	CACI	
EIDM	QSSI	
Infrastructure	Terremark & URS	
Help Desk	QuTech	
Testing Contractors	QSSI ACA, eGlobalTech	

Appointment

**From:** Jackson, Jeremy (CGI Federal) [Jeremy.Jackson@cgifederal.com]  
**Sent:** 8/6/2013 8:38:47 PM  
**To:** Zeiders, Chris (CGI Federal) [chris.zeiders@cgifederal.com]; Tor Flatebo [Tor.Flatebo@govdelivery.com]; Bobbie Browning (Bobbie.Browning@govdelivery.com) [Bobbie.Browning@govdelivery.com]; Tudor, Susan J. (CMS/OC) [Susan.J.Tudor@cms.gov]; Patel, Ketan (CMS/OC) [Ketan.Patel@cms.gov];  
[NotResp] [Redacted]; Rowe, Brandon L (CGI Federal) [brandon.rowe@cgifederal.com]; Banerjee, Dharitri (CGI Federal) [dharitri.banerjee@cgifederal.com]; Chandler, Adam (CGI Federal) [Adam.Chandler@cgifederal.com]; Wass, Stephen (CGI Federal) [Stephen.Wass@cgifederal.com]; Booth, Jon G. (CMS/OC) [Jon.G.Booth@cms.gov]; [NotResp] [Redacted]; Jackson, Jeremy (CGI Federal) [Jeremy.Jackson@cgifederal.com]

**Subject:** Review GovDelivery fixes

**Location:** (b)(6)

**Start:** 8/7/2013 1:30:00 PM

**End:** 8/7/2013 2:00:00 PM

**Show Time As:** Tentative

**Recurrence:** (none)

**Required Attendees:** Zeiders, Chris (CGI Federal); Tor Flatebo; Bobbie Browning (Bobbie.Browning@govdelivery.com); Tudor, Susan J. (CMS/OC); Patel, Ketan (CMS/OC); Rowe, Brandon L (CGI Federal); Banerjee, Dharitri (CGI Federal); Chandler, Adam (CGI Federal); Wass, Stephen (CGI Federal); Booth, Jon G. (CMS/OC)

We would like to review the following issues:

- \* Change GovDelivery redirector links from HTTP to HTTPS (see attached email) - this addresses a reported security issue
- \* Change GovDelivery TMS calls (e.g., email verification) to use new template (see attached email) - this improves our spam scores on TMS emails
- \* Support – and + in email names.

Email trail:

<<Re: TMS emails.>> <<RE: odlinks for healthcare.gov>> <<FW: List of Prioritized Fixes for Friday Lite Account Release>>

Thanks,

-JJ

Message

**From:** Health Insurance Marketplace [notices@healthcare.gov]  
**Sent:** 8/2/2013 7:01:42 PM  
**To:** Tor Flatebo [Tor.Flatebo@govdelivery.com]  
**Subject:** Confirm your Marketplace account

## Your Marketplace account has been created!

You must now click the link below to verify your email address.

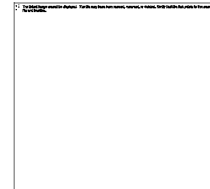
[Click this link to verify your email address](#)

If the above link does not work copy and paste the following verification URL into your web browser's address bar:

NotResp

You're receiving this message because you created an account with the Health Insurance Marketplace.

If you have questions or problems please visit <https://www.healthcare.gov/help-center/>.



Message

**From:** Jackson, Jeremy (CGI Federal) [Jeremy.Jackson@cgifederal.com]  
**Sent:** 8/6/2013 7:06:01 PM  
**To:** Tor Flatebo [Tor.Flatebo@govdelivery.com]; Bobbie Browning (Bobbie.Browning@govdelivery.com)  
 [Bobbie.Browning@govdelivery.com]; Tudor, Susan J. (CMS/OC) [NotResp]  
 [NotResp] Patel, Ketan (CMS/OC) [NotResp]  
 [NotResp] Booth, Jon G. (CMS/OC) [NotResp]  
**CC:** Zeiders, Chris (CGI Federal) [chris.zeiders@cgifederal.com]; Rowe, Brandon L (CGI Federal)  
 [brandon.rowe@cgifederal.com]; Banerjee, Dharitri (CGI Federal) [dharitri.banerjee@cgifederal.com]; Chandler,  
 Adam (CGI Federal) [Adam.Chandler@cgifederal.com]; Wass, Stephen (CGI Federal) [Stephen.Wass@cgifederal.com]  
**Subject:** FW: List of Prioritized Fixes for Friday Lite Account Release  
**Attachments:** RE: odlinks for healthcare.gov; Re: TMS emails.

Hi Tor,

We received the following issue list from CMS today involving the TMS service. Can we meet today or early tomorrow to discuss the possibility of implementing these changes highlighted below?

Let us know.

Thank you,  
 Jeremy Jackson | CGI Federal

**From:** booth, jon  
**Sent:** Tuesday, August 06, 2013 10:18 AM  
**To:** Winthrop, Monica (CGI Federal); Oh, Mark U. (CMS/OIS); Outerbridge, Monique (CMS/OIS); Schankweiler, Thomas W. (CMS/OIS); Chao, Henry (CMS/OIS); Peter Um; Calem, Mark (CGI Federal); Margush, Doug C. (CMS/OIS); thurston@sage-technologies.com; Patel, Ketan; Basavaraju, Venkat (CMS/OIS); Walter, Stephen J. (CMS/OIS); Shao, Lijun (CMS/CPI); Jackson, Jeremy (CGI Federal); Thurston, Robert (CMS/CTR); Rubin, Keith (CGI Federal); Zeiders, Chris (CGI Federal); Coutts, Todd (CMS/OIS); Royle, Erick B. (CMS/OIS); Dill, Walter (CMS/OIS); Thompson, Tyrone (CMS/OIS); lbjones@mitre.org  
**Cc:** Weiss, Paul (CGI Federal); Martin, Rich (CGI Federal); Gonzalez, Timothy J (CGI Federal); Ramamoorthy, Balaji Manikandan (CGI Federal); Gumma, Suresh (Non-Member); Alford, Justin (CGI Federal)  
**Subject:** List of Prioritized Fixes for Friday Lite Account Release

All,

Below is a prioritized list from OC of fixes & features for the Friday Lite Account release. Please let me know if you have questions on any of these or if CGI believes any of these can not be included.

Thanks,

Jon

1. Spanish launch (including all English fixes)
2. Address un-suppression
3. Change GovDelivery redirector links from HTTP to HTTPS (see attached email) - *this addresses a reported security issue*

4. Change GovDelivery TMS calls (e.g., email verification) to use new template (see attached email) - *this improves our spam scores on TMS emails*

5. Fix email verification timeout errors (allow full 48 hours) - *not sure if this is fully resolved but our testers have continued to report this sporadically*

6. UI edits:

- Header should not be sticky for Lite Account Launch
- There should be NO back button on the My Applications and Coverage page (nothing should be linkable)
- On the Account Settings page, the back button and person's name should take you back to the My Applications and Coverage
- There should be NO navy bar, just the baby blue bar

7. Content edits:

- On Login Page – “Sign Up” should read “Create Account”
- Error Message for Security Question – reads “This is not a valid Out of wallet answers.” - *should read "This is not a valid answer."*
- Verification Email – Should be a space and colon between the end of the sentence and verification URL

8. Inconsistency in coding for URLs. This is causing Google Analytics reporting issues and we are seeing application errors on certain paths only. - *OC will provide additional details and screenshots*



Message

**From:** Tor Flatebo [Tor.Flatebo@govdelivery.com]  
**Sent:** 8/2/2013 8:34:23 PM  
**To:** Booth, Jon G. (CMS/OC) [NotResp]  
 Patel, Ketan (CMS/OC) [NotResp]  
 Bobbie Browning [Bobbie.Browning@govdelivery.com]  
**CC:** Wright, Ltanya D. (CMS/OC) [NotResp]  
 [NotResp] Harris, Danielle Y. (CMS/OC) [NotResp]  
 [NotResp]  
**Subject:** Re: TMS emails.  
**Attachments:** CSMHIM\_TMS\_template\_responsive.html; Confirm your Marketplace account

Hi Jon,

I have attached a template that we designed based on the existing messages that are being sent through DCM. This template has a very low SPAM score of -0.16, vs. the 1.9 of the plain-text message that is currently being sent through TMS.

Also, this email template will work well across desktop email readers and mobile email readers, conforming to the screen size. This is a direction we are going with all of our email templates. I have attached an example of an email that was sent through TMS using this template.

You can see how the email renders in this Litmus report:  
<https://litmus.com/pub/590e129/screenshots>

We modified the wording in the account creation message to work well with email preview panes.

This template would be used to change the four messages that the Marketplace application sends through TMS. If your team needs any assistance with this template please let us know, we will be happy to help.

--

**Torleiv Flatebo** | Senior Technical Product Manager  
 p: (651) 379-6226 or (866) 276-5583 ext. 226 c: [Redacted]  
 Customer Support: 800.314.0147 | [help@govdelivery.com](mailto:help@govdelivery.com)

**From:** <Booth>, "Jon G. (CMS/OC)" <Jon.Booth@cms.hhs.gov>  
**Date:** Thursday, August 1, 2013 10:02 AM  
**To:** Torleiv Flatebo <tor.flatebo@govdelivery.com>, "Patel, Ketan (CMS/OC)" <Ketan.Patel@cms.hhs.gov>, Bobbie Browning <Bobbie.Browning@govdelivery.com>  
**Cc:** "Wright, Ltanya D. (CMS/OC)" <Ltanya.Wright@cms.hhs.gov>, "Harris, Danielle Y. (CMS/OC)" <Danielle.Harris@cms.hhs.gov>  
**Subject:** Re: TMS emails.

Thanks, got it. If you can send us the template I will work with our developers to schedule the change with the next hot fix.

**From:** Tor Flatebo <[Tor.Flatebo@govdelivery.com](mailto:Tor.Flatebo@govdelivery.com)>

**Date:** Thursday, August 1, 2013 10:55 AM

**To:** Jon Booth <[jon.booth@cms.hhs.gov](mailto:jon.booth@cms.hhs.gov)>, Ketan Patel BB <[Ketan.Patel@cms.hhs.gov](mailto:Ketan.Patel@cms.hhs.gov)>, Bobbie Browning <[Bobbie.Browning@govdelivery.com](mailto:Bobbie.Browning@govdelivery.com)>

**Cc:** "Wright, Ltanya D. (CMS/OC)" <[Ltanya.Wright@cms.hhs.gov](mailto:Ltanya.Wright@cms.hhs.gov)>, Danielle Harris BB <[Danielle.Harris@cms.hhs.gov](mailto:Danielle.Harris@cms.hhs.gov)>

**Subject:** Re: TMS emails.

Hi Jon,

We cannot deploy the template on my side in GovDelivery TMS, as the content of the TMS emails are controlled by your application when you send to TMS.

So unless the template is deployed into your application, we cannot change the layout of the messages.

--

**Torleiv Flatebo** | Senior Technical Product Manager

p: (651) 379-6226 or (866) 276-5583 ext. 226 f: (651) 665-0943

Customer Support: 800.314.0147 | [help@govdelivery.com](mailto:help@govdelivery.com)

**From:** <Booth>, "Jon G. (CMS/OC)" <[Jon.Booth@cms.hhs.gov](mailto:Jon.Booth@cms.hhs.gov)>

**Date:** Thursday, August 1, 2013 9:52 AM

**To:** Torleiv Flatebo <[tor.flatebo@govdelivery.com](mailto:tor.flatebo@govdelivery.com)>, "Patel, Ketan (CMS/OC)" <[Ketan.Patel@cms.hhs.gov](mailto:Ketan.Patel@cms.hhs.gov)>, Bobbie Browning <[Bobbie.Browning@govdelivery.com](mailto:Bobbie.Browning@govdelivery.com)>

**Cc:** "Wright, Ltanya D. (CMS/OC)" <[Ltanya.Wright@cms.hhs.gov](mailto:Ltanya.Wright@cms.hhs.gov)>, "Harris, Danielle Y. (CMS/OC)" <[Danielle.Harris@cms.hhs.gov](mailto:Danielle.Harris@cms.hhs.gov)>

**Subject:** Re: TMS emails.

Thanks, that does answer my question.

We would likely make the change as part of a hot fix next week rather than make this change now. Would the current (unchanged) API calls break if you deploy this template, or will they continue to work?

**From:** Tor Flatebo <[Tor.Flatebo@govdelivery.com](mailto:Tor.Flatebo@govdelivery.com)>

**Date:** Thursday, August 1, 2013 10:50 AM

**To:** Jon Booth <[jon.booth@cms.hhs.gov](mailto:jon.booth@cms.hhs.gov)>, Ketan Patel BB <[Ketan.Patel@cms.hhs.gov](mailto:Ketan.Patel@cms.hhs.gov)>, Bobbie Browning <[Bobbie.Browning@govdelivery.com](mailto:Bobbie.Browning@govdelivery.com)>

**Cc:** "Wright, Ltanya D. (CMS/OC)" <[Ltanya.Wright@cms.hhs.gov](mailto:Ltanya.Wright@cms.hhs.gov)>, Danielle Harris BB <[Danielle.Harris@cms.hhs.gov](mailto:Danielle.Harris@cms.hhs.gov)>

**Subject:** Re: TMS emails.

Hi Jon,

The structure of the API calls themselves, and how the API is called will not need to change.

The entire content of the emails send throughout TMS are provided in each API call, so the template I send you will need to be installed into your application and used each time the API call is made.

I am not particularly familiar with the FFM application so I cannot say what type of change is needed, but something will need to change in the Marketplace application to use the new template.

Does that answer your question?

--

**Torleiv Flatebo** | Senior Technical Product Manager  
p: (651) 379-6226 or (866) 276-5583 ext. 226 f: (651) 665-0943  
Customer Support: 800.314.0147 | [help@govdelivery.com](mailto:help@govdelivery.com)

**From:** <Booth>, "Jon G. (CMS/OC)" <[Jon.Booth@cms.hhs.gov](mailto:Jon.Booth@cms.hhs.gov)>  
**Date:** Thursday, August 1, 2013 9:22 AM  
**To:** Torleiv Flatebo <[tor.flatebo@govdelivery.com](mailto:tor.flatebo@govdelivery.com)>, "Patel, Ketan (CMS/OC)" <[Ketan.Patel@cms.hhs.gov](mailto:Ketan.Patel@cms.hhs.gov)>, Bobbie Browning <[Bobbie.Browning@govdelivery.com](mailto:Bobbie.Browning@govdelivery.com)>  
**Cc:** "Wright, Ltanya D. (CMS/OC)" <[Ltanya.Wright@cms.hhs.gov](mailto:Ltanya.Wright@cms.hhs.gov)>, "Harris, Danielle Y. (CMS/OC)" <[Danielle.Harris@cms.hhs.gov](mailto:Danielle.Harris@cms.hhs.gov)>  
**Subject:** Re: TMS emails.

Thanks. To your 3rd point, does this mean API calls need to be modified or is this automatic?

**From:** Tor Flatebo <[Tor.Flatebo@govdelivery.com](mailto:Tor.Flatebo@govdelivery.com)>  
**Date:** Thursday, August 1, 2013 10:20 AM  
**To:** Jon Booth <[jon.booth@cms.hhs.gov](mailto:jon.booth@cms.hhs.gov)>, Ketan Patel BB <[Ketan.Patel@cms.hhs.gov](mailto:Ketan.Patel@cms.hhs.gov)>, Bobbie Browning <[Bobbie.Browning@govdelivery.com](mailto:Bobbie.Browning@govdelivery.com)>  
**Cc:** "Wright, Ltanya D. (CMS/OC)" <[Ltanya.Wright@cms.hhs.gov](mailto:Ltanya.Wright@cms.hhs.gov)>, Danielle Harris BB <[Danielle.Harris@cms.hhs.gov](mailto:Danielle.Harris@cms.hhs.gov)>  
**Subject:** Re: TMS emails.

Hi Jon,

The next steps here:

1. GovDelivery provides you with a template
2. That template will be installed into your application that uses TMS
3. The template is provided in the API call to TMS for each send

--

**Torleiv Flatebo** | Senior Technical Product Manager  
p: (651) 379-6226 or (866) 276-5583 ext. 226 f: (651) 665-0943  
Customer Support: 800.314.0147 | [help@govdelivery.com](mailto:help@govdelivery.com)

**From:** Torleiv Flatebo <[tor.flatebo@govdelivery.com](mailto:tor.flatebo@govdelivery.com)>

**Date:** Thursday, August 1, 2013 9:00 AM

**To:** "Booth, Jon G. (CMS/OC)" <[Jon.Booth@cms.hhs.gov](mailto:Jon.Booth@cms.hhs.gov)>, "Patel, Ketan (CMS/OC)" <[Ketan.Patel@cms.hhs.gov](mailto:Ketan.Patel@cms.hhs.gov)>, Bobbie Browning <[Bobbie.Browning@govdelivery.com](mailto:Bobbie.Browning@govdelivery.com)>

**Cc:** "Wright, Ltanya D. (CMS/OC)" <[Ltanya.Wright@cms.hhs.gov](mailto:Ltanya.Wright@cms.hhs.gov)>, "Harris, Danielle Y. (CMS/OC)" <[Danielle.Harris@cms.hhs.gov](mailto:Danielle.Harris@cms.hhs.gov)>

**Subject:** Re: TMS emails.

Hi Jon,

We will provide you with a template. I will get one over to you ASAP.

--

**Torleiv Flatebo** | Senior Technical Product Manager

p: (651) 379-6226 or (866) 276-5583 ext. 226 f: (651) 665-0943

Customer Support: 800.314.0147 | [help@govdelivery.com](mailto:help@govdelivery.com)

**From:** <Booth>, "Jon G. (CMS/OC)" <[Jon.Booth@cms.hhs.gov](mailto:Jon.Booth@cms.hhs.gov)>

**Date:** Thursday, August 1, 2013 8:53 AM

**To:** Torleiv Flatebo <[tor.flatebo@govdelivery.com](mailto:tor.flatebo@govdelivery.com)>, "Patel, Ketan (CMS/OC)" <[Ketan.Patel@cms.hhs.gov](mailto:Ketan.Patel@cms.hhs.gov)>, Bobbie Browning <[Bobbie.Browning@govdelivery.com](mailto:Bobbie.Browning@govdelivery.com)>

**Cc:** "Wright, Ltanya D. (CMS/OC)" <[Ltanya.Wright@cms.hhs.gov](mailto:Ltanya.Wright@cms.hhs.gov)>, "Harris, Danielle Y. (CMS/OC)" <[Danielle.Harris@cms.hhs.gov](mailto:Danielle.Harris@cms.hhs.gov)>

**Subject:** Re: TMS emails.

Tor,

We'd like to proceed with option 3. Can you let me know next steps that make that happen?

Thanks,

Jon

**From:** Tor Flatebo <[Tor.Flatebo@govdelivery.com](mailto:Tor.Flatebo@govdelivery.com)>

**Date:** Wednesday, July 31, 2013 5:56 PM

**To:** Ketan Patel BB <[Ketan.Patel@cms.hhs.gov](mailto:Ketan.Patel@cms.hhs.gov)>, Bobbie Browning <[Bobbie.Browning@govdelivery.com](mailto:Bobbie.Browning@govdelivery.com)>

**Cc:** Jon Booth <[jon.booth@cms.hhs.gov](mailto:jon.booth@cms.hhs.gov)>, "Wright, Ltanya D. (CMS/OC)" <[Ltanya.Wright@cms.hhs.gov](mailto:Ltanya.Wright@cms.hhs.gov)>, Danielle Harris BB <[Danielle.Harris@cms.hhs.gov](mailto:Danielle.Harris@cms.hhs.gov)>

**Subject:** Re: TMS emails.

Hello Ketan,

After doing additional analysis on the TMS emails, we found the following:

1. SPAM scores are relatively low on these emails in their current state

2. Using opens and link encoding is biggest hit right now combined with the small amount of text
3. In general, deliverability and inbox placement is at or above 92% in the current state of the message
4. DCM welcome transactional emails have a very low SPAM score and 100% inbox placement due to proper balance of text and pictures

**(Recommended) Option 1:** Disable open and link tracking on TMS emails until further work can be done on the content and formatting of the TMS emails

To do this, the API calls into TMS made by CMS/CGI will need to have these two values set to "false": "open\_tracking\_enabled":"false", "click\_tracking\_enabled":"false"

**Option 2:** Do nothing and leave the messages as is. The inbox placement is actually much higher than the industry average of around 80-85%

**Option 3:** We can provide a template for the TMS emails that will be similar to DCM emails to get a much lower SPAM score

If Option 1 isn't possible in the very short term, adding content to the emails or disabling open tracking will have an appreciable impact on inbox placement. We feel that developing additional content in these emails is the way to get the inbox placement as high as possible and can work with you to get those templates in place.

Inbox placement can vary across ISPs and even based on previous user behavior. Your users may be seeing SPAM folder hits due to their behavior with the sending domain in the past, as ISPs are moving to behavior based scoring.

Please let us know if we can assist you in any way.

--

**Torleiv Flatebo** | Senior Technical Product Manager

p: (651) 379-6226 or (866) 276-5583 ext. 226 f: (651) 665-0943

Customer Support: 800.314.0147 | [help@govdelivery.com](mailto:help@govdelivery.com)

**From:** Torleiv Flatebo <[tor.flatebo@govdelivery.com](mailto:tor.flatebo@govdelivery.com)>

**Date:** Wednesday, July 31, 2013 10:09 AM

**To:** "Patel, Ketan (CMS/OC)" <[Ketan.Patel@cms.hhs.gov](mailto:Ketan.Patel@cms.hhs.gov)>, Bobbie Browning <[Bobbie.Browning@govdelivery.com](mailto:Bobbie.Browning@govdelivery.com)>

**Cc:** "Booth, Jon G. (CMS/OC)" <[Jon.Booth@cms.hhs.gov](mailto:Jon.Booth@cms.hhs.gov)>, "Wright, Ltanya D. (CMS/OC)" <[Ltanya.Wright@cms.hhs.gov](mailto:Ltanya.Wright@cms.hhs.gov)>, "Harris, Danielle Y. (CMS/OC)" <[Danielle.Harris@cms.hhs.gov](mailto:Danielle.Harris@cms.hhs.gov)>

**Subject:** Re: TMS emails.

Hi Ketan,

Thank you for providing the headers. We will do some more testing and get back to you.

--

**Torleiv Flatebo** | Senior Technical Product Manager

p: (651) 379-6226 or (866) 276-5583 ext. 226 f: (651) 665-0943



**From:** <Patel>, "Ketan (CMS/OC)" <[Ketan.Patel@cms.hhs.gov](mailto:Ketan.Patel@cms.hhs.gov)>

**Date:** Wednesday, July 31, 2013 10:04 AM

**To:** Torleiv Flatebo <[tor.flatebo@govdelivery.com](mailto:tor.flatebo@govdelivery.com)>, Bobbie Browning <[Bobbie.Browning@govdelivery.com](mailto:Bobbie.Browning@govdelivery.com)>

**Cc:** "Booth, Jon G. (CMS/OC)" <[Jon.Booth@cms.hhs.gov](mailto:Jon.Booth@cms.hhs.gov)>, "Wright, Ltanya D. (CMS/OC)" <[Ltanya.Wright@cms.hhs.gov](mailto:Ltanya.Wright@cms.hhs.gov)>, "Harris, Danielle Y. (CMS/OC)" <[Danielle.Harris@cms.hhs.gov](mailto:Danielle.Harris@cms.hhs.gov)>

**Subject:** Re: TMS emails.

See attached hotmail recent example.

**From:** Tor Flatebo <[Tor.Flatebo@govdelivery.com](mailto:Tor.Flatebo@govdelivery.com)>

**Date:** Tuesday, July 30, 2013 5:50 PM

**To:** Ketan PATEL <[ketan.patel@cms.hhs.gov](mailto:ketan.patel@cms.hhs.gov)>, Bobbie Browning <[Bobbie.Browning@govdelivery.com](mailto:Bobbie.Browning@govdelivery.com)>

**Cc:** Jon Booth BB <[Jon.Booth@cms.hhs.gov](mailto:Jon.Booth@cms.hhs.gov)>, Ltanya Wright <[LTANYA.WRIGHT@CMS.HHS.GOV](mailto:LTANYA.WRIGHT@CMS.HHS.GOV)>, "HARRIS, (CMS/OBIS)" <[Danielle.Harris@cms.hhs.gov](mailto:Danielle.Harris@cms.hhs.gov)>

**Subject:** Re: TMS emails.

Hello Ketan,

We have done some analysis here on the email being sent via GovDelivery TMS. We have a tool that tests inbox placement, and initial results using that tool are positive.

1. **98%** of the emails were delivered to the inbox
2. Only Yahoo showed the emails as being delivered to the SPAM folder
3. Our seed list covers covers 20 major ISPs and major SPAM filters

The rule that was marked as triggering the SPAM filter in Yahoo was this:

HTML: images with 1200-1600 bytes of words - This indicates there is too much text written into the images in the email. Spammers have used images to hide spammy or offensive language. (rule-id: 67)

This rule indicates that the body of the email doesn't include enough text for the one image that is included in the message. The image in the message is the open tracking (invisible) gif. Including more text in the message will cause this rule to not fire. Alternatively, open tracking can be disabled on the TMS messages.

I am sending more tests using our tool to ensure that the data reported here is completely accurate. I will send more information if the results of further tests are different than this.

--

**Torleiv Flatebo** | Senior Technical Product Manager

p: (651) 379-6226 or (866) 276-5583 ext. 226 f: (651) 665-0943

Customer Support: 800.314.0147 | [help@govdelivery.com](mailto:help@govdelivery.com)

**From:** <Patel>, "Ketan (CMS/OC)" <[Ketan.Patel@cms.hhs.gov](mailto:Ketan.Patel@cms.hhs.gov)>

**Date:** Monday, July 29, 2013 2:35 PM

**To:** Torleiv Flatebo <[tor.flatebo@govdelivery.com](mailto:tor.flatebo@govdelivery.com)>, Bobbie Browning <[Bobbie.Browning@govdelivery.com](mailto:Bobbie.Browning@govdelivery.com)>  
**Cc:** "Booth, Jon G. (CMS/OC)" <[Jon.Booth@cms.hhs.gov](mailto:Jon.Booth@cms.hhs.gov)>, "Wright, Ltanya D. (CMS/OC)" <[Ltanya.Wright@cms.hhs.gov](mailto:Ltanya.Wright@cms.hhs.gov)>, "Harris, Danielle Y. (CMS/OC)" <[Danielle.Harris@cms.hhs.gov](mailto:Danielle.Harris@cms.hhs.gov)>  
**Subject:** RE: TMS emails.

Yes both in spam folder.

**From:** Tor Flatebo [<mailto:Tor.Flatebo@govdelivery.com>]  
**Sent:** Monday, July 29, 2013 3:26 PM  
**To:** Patel, Ketan (CMS/OC); Bobbie Browning  
**Cc:** Booth, Jon G. (CMS/OC); Wright, Ltanya D. (CMS/OC); Harris, Danielle Y. (CMS/OC)  
**Subject:** Re: TMS emails.

Hi Ketan,

Thank you. And to confirm these are showing up in your SPAM folder (both examples you sent me)?

--

**Torleiv Flatebo** | Senior Technical Product Manager  
p: (651) 379-6226 or (866) 276-5583 ext. 226 f: (651) 665-0943  
Customer Support: 800.314.0147 | [help@govdelivery.com](mailto:help@govdelivery.com)

**From:** <Patel>, "Ketan (CMS/OC)" <[Ketan.Patel@cms.hhs.gov](mailto:Ketan.Patel@cms.hhs.gov)>  
**Date:** Monday, July 29, 2013 2:22 PM  
**To:** Torleiv Flatebo <[tor.flatebo@govdelivery.com](mailto:tor.flatebo@govdelivery.com)>, Bobbie Browning <[Bobbie.Browning@govdelivery.com](mailto:Bobbie.Browning@govdelivery.com)>  
**Cc:** "Booth, Jon G. (CMS/OC)" <[Jon.Booth@cms.hhs.gov](mailto:Jon.Booth@cms.hhs.gov)>, "Wright, Ltanya D. (CMS/OC)" <[Ltanya.Wright@cms.hhs.gov](mailto:Ltanya.Wright@cms.hhs.gov)>, "Harris, Danielle Y. (CMS/OC)" <[Danielle.Harris@cms.hhs.gov](mailto:Danielle.Harris@cms.hhs.gov)>  
**Subject:** RE: TMS emails.

Tor Yahoo version of the header I tested this against prod system test.

Thanks,  
Ketan

**From:** Tor Flatebo [<mailto:Tor.Flatebo@govdelivery.com>]  
**Sent:** Monday, July 29, 2013 12:08 PM  
**To:** Patel, Ketan (CMS/OC); Bobbie Browning  
**Cc:** Booth, Jon G. (CMS/OC); Wright, Ltanya D. (CMS/OC); Harris, Danielle Y. (CMS/OC)  
**Subject:** Re: TMS emails.

Hello Ketan,

Thank you this is helpful. We will investigate this and get back to you.

---  
**Torleiv Flatebo** | Senior Technical Product Manager  
p: (651) 379-6226 or (866) 276-5583 ext. 226 f: (651) 665-0943  
Customer Support: 800.314.0147 | [help@govdelivery.com](mailto:help@govdelivery.com)

**From:** <Patel>, "Ketan (CMS/OC)" <[Ketan.Patel@cms.hhs.gov](mailto:Ketan.Patel@cms.hhs.gov)>  
**Date:** Monday, July 29, 2013 9:58 AM  
**To:** Torleiv Flatebo <[tor.flatebo@govdelivery.com](mailto:tor.flatebo@govdelivery.com)>, Bobbie Browning <[Bobbie.Browning@govdelivery.com](mailto:Bobbie.Browning@govdelivery.com)>  
**Cc:** "Booth, Jon G. (CMS/OC)" <[Jon.Booth@cms.hhs.gov](mailto:Jon.Booth@cms.hhs.gov)>, "Wright, Ltanya D. (CMS/OC)" <[Ltanya.Wright@cms.hhs.gov](mailto:Ltanya.Wright@cms.hhs.gov)>, "Harris, Danielle Y. (CMS/OC)" <[Danielle.Harris@cms.hhs.gov](mailto:Danielle.Harris@cms.hhs.gov)>  
**Subject:** RE: TMS emails.

Hotmail Header.

**From:** Tor Flatebo [<mailto:Tor.Flatebo@govdelivery.com>]  
**Sent:** Monday, July 29, 2013 10:50 AM  
**To:** Patel, Ketan (CMS/OC); Bobbie Browning  
**Cc:** Booth, Jon G. (CMS/OC); Wright, Ltanya D. (CMS/OC); Harris, Danielle Y. (CMS/OC)  
**Subject:** Re: TMS emails.  
**Importance:** High

Hello Ketan,

Can you have anyone who is experiencing this send me the emails that are landing in SPAM folders **with headers** so that we can inspect them? This would help us to diagnose the issues.

Here is how to do send the whole message body with headers across different email clients:  
<https://support.google.com/mail/answer/22454?hl=en>

Also:

1. Did this just start happening?
2. Has this happened before?
3. Are there specific ISPs that are sending these messages to SPAM?

If there are any questions about how to include the headers, please contact me.

---  
**Torleiv Flatebo** | Senior Technical Product Manager  
p: (651) 379-6226 or (866) 276-5583 ext. 226 f: (651) 665-0943  
Customer Support: 800.314.0147 | [help@govdelivery.com](mailto:help@govdelivery.com)

**From:** <Patel>, "Ketan (CMS/OC)" <[Ketan.Patel@cms.hhs.gov](mailto:Ketan.Patel@cms.hhs.gov)>  
**Date:** Monday, July 29, 2013 8:46 AM

**To:** Bobbie Browning <[Bobbie.Browning@govdelivery.com](mailto:Bobbie.Browning@govdelivery.com)>, Torleiv Flatebo <[tor.flatebo@govdelivery.com](mailto:tor.flatebo@govdelivery.com)>

**Cc:** "Booth, Jon G. (CMS/OC)" <[Jon.Booth@cms.hhs.gov](mailto:Jon.Booth@cms.hhs.gov)>, "Wright, Ltanya D. (CMS/OC)" <[Ltanya.Wright@cms.hhs.gov](mailto:Ltanya.Wright@cms.hhs.gov)>, "Harris, Danielle Y. (CMS/OC)" <[Danielle.Harris@cms.hhs.gov](mailto:Danielle.Harris@cms.hhs.gov)>

**Subject:** TMS emails.

We are seeing lots of people complaining about emails sent via TMS for lite account testing are going to Junk mail box.

Any insight into that.

- 1) <!--[if !supportLists]--><!--[endif]-->Is it message header
- 2) <!--[if !supportLists]--><!--[endif]-->Is it message content

Thanks,  
Ketan

## Your Marketplace account has been created!

You must now click the link below to verify your email address.

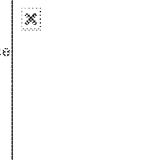
[Click this link to verify your email address](#)

If the above link does not work copy and paste the following verification URL into your web browser's address bar:

**NotResp**

You're receiving this message because you created an account with the Health Insurance Marketplace.

If you have questions or problems please visit <https://www.healthcare.gov/help-center/>.



Message

**From:** Health Insurance Marketplace [notices@healthcare.gov]  
**Sent:** 8/2/2013 7:01:42 PM  
**To:** Tor Flatebo [Tor.Flatebo@govdelivery.com]  
**Subject:** Confirm your Marketplace account

## Your Marketplace account has been created!

You must now click the link below to verify your email address.

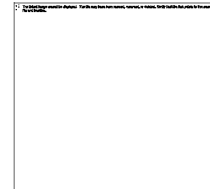
[Click this link to verify your email address](#)

If the above link does not work copy and paste the following verification URL into your web browser's address bar:

NotResp

You're receiving this message because you created an account with the Health Insurance Marketplace.

If you have questions or problems please visit <https://www.healthcare.gov/help-center/>.



Appointment

**From:** Hoffman, Jessica (CMS/OIS) [NotResp]  
 [NotResp]  
**Sent:** 5/8/2014 4:19:37 PM  
**To:** Hoffman, Jessica (CMS/OIS) [NotResp]  
 Lyles, Darrin V. (CMS/OIS) [NotResp]  
 [NotResp] Tran1 Minh Q. (CMS/CTR) [NotResp]  
 [NotResp] 'CMS\_PMO'  
 [NotResp] bluecanopy.com]; Patel, Ketan (CMS/OC) [NotResp]  
 [NotResp] Le, Thao Q. (CMS/OC) [NotResp]  
 [NotResp]; CMS - WNMG\_Security [NotResp]  
 [NotResp]; King, Jason C. (CMS/OIS) [NotResp]  
 [NotResp]; Hemby, Kimberly R. (CMS/OIS) [NotResp]  
 [NotResp]  
**Subject:** Finder.Healthcare.Gov SCA Preliminary Discussion  
**Start:** 5/13/2014 6:00:00 PM  
**End:** 5/13/2014 7:00:00 PM  
**Show Time As:** Tentative

**Required** Lyles, Darrin V. (CMS/OIS); Tran1 Minh Q. (CMS/CTR); 'CMS\_PMO'; Patel, Ketan (CMS/OC); Le, Thao Q. (CMS/OC);  
**Attendees:** CMS - WNMG\_Security; King, Jason C. (CMS/OIS) (Jason.King@cms.hhs.gov); Hemby, Kimberly R. (CMS/OIS)

OC, please forward to the rest of your support team. Thanks!

AGENDA

- Intro
- Brief Description of the Systems Purpose & Functionality
- Brief Overview of Operational Environment (Location, Application Development language, Database, Interconnections, etc)
- Security Assessment Process and Assessment Methodology
- Scoping: Determine the Boundaries of the Test
- Timeframe & Scheduling
- Identify CMS POCs, ISSO, Business Owner, and Testing Team
- Required Documentation
- Application Access Requirements (EUA, IACS, etc)
- Testing Requirements, Expectations and Special Security Concerns
- Questions, Issues and/or Concerns
- Next Steps and Meeting scheduled Date (Draft Test Plan)

Jessica Hoffman invites you to an online meeting using WebEx.

Meeting Number: (b)(6)

Meeting Password: Please obtain your meeting password from your host.



-----  
Audio conference information  
-----

1. Please call the following number:

WebEx: (b)(6)

2. Follow the instructions you hear on the phone.

Your WebEx Meeting Number: (b)(6)

-----  
To join from a Cisco VoIP enabled CMS Region or from CMS Central Office  
-----

1. Dial ext: (b)(6)

2. Enter the Meeting Number: (b)(6)

-----  
To join this meeting online  
-----

1. Go to [https://\(b\)\(6\)](https://(b)(6))

2. If requested, enter your name and email address.

3. If a password is required, enter the meeting password: Please obtain your meeting password from your host.

4. Click "Join".

5. Follow the instructions that appear on your screen.

Appointment

**From:** Schankweiler, Thomas W. (CMS/OIS) [NotResp]  
[NotResp]

**Sent:** 3/14/2014 7:02:27 PM

**To:** Schankweiler, Thomas W. (CMS/OIS) [NotResp]  
[NotResp]; CMS - Marketplace Security Team [NotResp]  
[NotResp]  
[NotResp] Quaintance, Eric (CGI Federal) [Eric.Quaintance@cgifederal.com]; Customer Care at Akamai [ccare@akamai.com]; Patel, Ketan (CMS/OC) [NotResp]  
[NotResp] Booth, Jon G. (CMS/OC) [NotResp]  
[NotResp] -cms@akamai.com; sifr@akamai.com; Boden, John (CMS/CTR) [NotResp]  
[NotResp] Millheiser, Robert [rmmiller@akamai.com; 'dboeckman@qssinc.com'; 'dboeckman@qssinc.com']

**Subject:** Quick call on NY Traffic

**Location:** Con call

**Start:** 3/14/2014 7:05:00 PM

**End:** 3/14/2014 7:35:00 PM

**Show Time As:** Tentative

**Recurrence:** (none)

**Required Attendees:** CMS - Marketplace Security Team; Quaintance, Eric (CGI Federal); Customer Care at Akamai; Patel, Ketan (CMS/OC); Booth, Jon G. (CMS/OC); pubsec-cms@akamai.com; sifr@akamai.com; Boden, John (CMS/CTR); Millheiser, Robert; 'dboeckman@qssinc.com'

Hello all,

Can you join a quick call about this NY traffic?

CMS team,

Today we saw suspicious activity from [NotResp] Cablevision, Brooklyn NY). It might be batch processing but it's from a cable operator IP and all recent activity was directed against a specific .cgi . Please let us know if this is malicious or not, but it has the indicators of a brute force attack against the registration page.

The Referer is: [https://www.healthcare.gov/marketplace/global/en\\_US/registration](https://www.healthcare.gov/marketplace/global/en_US/registration)

<eidm.cms.gov/obrar.cgi>

Note fro Eric:

The \*cgi endpoints in question are OAM (EIDM). They're requested in a particular sequence during the authentication process. The garbage strings are encrypted and partially URL encoded.

The detail in this thread is insufficient to make an assessment of any potential foul play. If Akamai has observed a higher volume here, indicative of a brute force or DoS, perhaps they and MST can check out the username and password

parameters being POSTed to another surrounding endpoint NotRes  
p server/authentication?type=English to help out with that determination.

Thomas Schankweiler invites you to an online meeting using WebEx.

Meeting Number: (b)(6)

Meeting Password: This meeting does not require a password.

---

Audio conference information

---

1. Please call the following number:

WebEx (b)(6)

2. Follow the instructions you hear on the phone.

Your WebEx Meeting Number: (b)(6)

---

To join from a Cisco VoIP enabled CMS Region or from CMS Central Office

---

1. Dial ext (b)(6)

2. Enter the Meeting Number (b)(6)

---

To join this meeting online

---

1. Go to [\(b\)\(6\)">https://\(b\)\(6\)](https://<span style=)

2. If requested, enter your name and email address.

3. If a password is required, enter the meeting password: This meeting does not require a password.

4. Click "Join".

5. Follow the instructions that appear on your screen.

## Appointment

**From:** Walker, Erin S (CGI Federal) [erin.walker@cgifederal.com]  
**Sent:** 2/5/2013 6:10:08 PM  
**To:** Patel, Ketan (CMS/OC); [Redacted] NotResp  
 Tudor, Susan J. (CMS/OC) [Redacted] NotResp  
 [Redacted] NotResp; Nate Mudd (natemudd@gmail.com) [natemudd@gmail.com];  
 Booth, Jon G. (CMS/OC); [Redacted] NotResp  
**Subject:** FW: Primary / Secondary Clarification  
**Location:** Conference Bridge  
**Start:** 2/5/2013 6:30:00 PM  
**End:** 2/5/2013 7:00:00 PM  
**Show Time As:** Tentative  
**Recurrence:** (none)  
**Required Attendees:** Tudor, Susan J. (CMS/OC); Nate Mudd (natemudd@gmail.com); Patel, Ketan (CMS/OC); Booth, Jon G. (CMS/OC)

Not sure if any of you have bandwidth to join this meeting with CGI and CCIO; they are looking to discuss what OC's issues are with the Primary vs. Secondary categorizations in the "expedited" schedule. Here's what they've provided us to date:

## 1.) Primary Flow:

- \* The Primary Flow focuses on UI enhancements to the Low Fidelity wireframes depicting current User Stories and Requirements. These enhancements will result from a progression from Low Fidelity Wireframes, to Annotated Wireframes, to High Fidelity Wireframes to UI Specs (including Mock Ups).
- \* The Primary Flow allows the user to navigate from the start of the module to the end of the module (with edit support) for all easy and complex paths
- \* The Primary Flow is the core functionality to make the module "work" and enable testing (stress, Partner, State, etc ...).
- \* Note: For Architecture reasons the Primary flow will also cover item 36 on the Shepherding tab for system down handling.

2.) Secondary Flow: I've also attached the latest snapshot of the open issues list which reflects the horizontal and shepherding details (tabs respectively). The table below represents a subset.

- \* The Secondary Flow improves the User Experience by layering additional functionality to guide users through the applications.
- \* The Secondary Flow will focus on Shepherding and Horizontal items (see Tabs in attached EE UI Apps Open Questions).
- \* The scheduling difference between the Primary Flow and Secondary Flow will allow time for a baseline to be established that can then be enhanced and rolled out to for consistency cross module and for dependencies to be met.

Category	Item	Dependency
Horizontal	Headers and Footers	- Healthcare.gov
	State Branding Requirements	
	Help (Glossary, Learn More, Tool Tips, How did we get this information, Chat) and Educational Content	- Percussion
Integration	Content	
	Contact Information	- Healthcare.gov (for example Navigators and State Programs)
	Submit/Upload	- Cross module integration (Individual Application, MyAccount, Plan Compare, SHOP)

- Technical Design
    - Print/Download - Cross module integration (Individual Application, MyAccount, Plan Compare, SHOP)
  - Technical Design
    - GovDelivery - Healthcare.gov
    - URL structure - Healthcare.gov
    - User Feedback - Healthcare.gov
    - Social Media - Healthcare.gov
    - Additional Languages - Healthcare.gov
    - Search - Healthcare.gov
    - Inconsistency Analysis of Global Styles and Design Patterns - Finalized Visual Design Style Guide
- Shepherding
- To Do Lists - Cross module integration (Individual Application, MyAccount, Plan Compare, SHOP)
  - Progress Bars - Cross module integration (Individual Application, MyAccount, Plan Compare, SHOP)
  - Instructional Pages (Chapter, Section, Cover) - Content
  - State Routing (including ability for Users to Change State) - Healthcare.gov
  - Cross module integration (Individual Application, MyAccount, Plan Compare, SHOP)
  - Calculators - Healthcare.gov (examples: Out-of-Pocket, Household Income)
  - Decision Support Tools - Healthcare.gov (example: APTC)

-----Original Appointment-----

From: Walker, Erin S (CGI Federal) [<mailto:erin.walker@cgifederal.com>]

Sent: Tuesday, February 05, 2013 12:28 PM

To: Walker, Erin S (CGI Federal); Moore, Hannah Y. (CMS/CCIIO); Amos, Robert E. (CMS/OC); Trefzger, William (CMS/DWO); Weiss, Paul (CGI Federal); Waple, Elisabeth (CGI Federal); Martin, Kyle (CGI Federal); Jarding, Andrew (Non-Member); Rowe, Brandon L (CGI Federal); Tomjack, Florence G (CGI Federal); Jackson, Jeremy (CGI Federal)

Subject: Primary / Secondary Clarification

When: Tuesday, February 05, 2013 1:30 PM-2:00 PM (UTC-05:00) Eastern Time (US & Canada).

Where: Conference Bridge

For access to MeetingPlace via the web site: <http://meet.cgifederal.com> <<http://meet.cgifederal.com/>>

Dial In: (b)(6)

Passcode: (b)(6)

Appointment

**From:** Patel, Ketan (CMS/OC) [NotResp]  
[NotResp]

**Sent:** 2/20/2014 9:22:57 PM

**To:** Patel, Ketan (CMS/OC) [NotResp]  
pubsec-cms@akamai.com; Mudumby, Ravi (Ravi.Mudumby@aquilent.com) [Ravi.Mudumby@aquilent.com]; Newhouse, Andrew (Andrew.Newhouse@aquilent.com) [Andrew.Newhouse@aquilent.com]; Osborne, Joe [joe.osborne@aquilent.com]; 'alex.westholm@alextom.com' (alex.westholm@alextom.com) [alex.westholm@alextom.com]; Maimudar, Vidit S. (CMS/OC) [NotResp]  
[NotResp] matt.simpson@alextom.com  
(matt.simpson@alextom.com) [matt.simpson@alextom.com]; Mudd, Nathaniel (CMS/OC) [NotResp]  
[NotResp] CMS - WNMG\_Security [NotResp]  
[NotResp] Warren, Kevin (CMS/OIS) [NotResp]  
[NotResp]

**CC:** Millheiser, Robert [rmillhei@akamai.com]

**Subject:** Discuss Search.Healthcare.gov security issues.

**Location:** Ketan's or call in

**Start:** 2/20/2014 10:00:00 PM

**End:** 2/20/2014 10:30:00 PM

**Show Time As:** Tentative

**Importance:** High

**Recurrence:** (none)

Scanned document 20-02-2014 15-51-15.pdf

+-----+

[Do not add or change anything below this line. The information in this section may be replaced with your meeting details after you click Send.]

You scheduled this meeting.

Meeting Number: (b)(6)

Meeting Password: This meeting does not require a password.

Audio conference information

1. Please call the following number:

WebEx (b)(6)

2. Follow the instructions you hear on the phone.

Your WebEx Meeting Number: (b)(6)

-----  
To join from a Cisco VoIP enabled CMS Region or from CMS Central Office  
-----

1. Dial ext. (b)(6)
  2. Enter the Meeting Number: (b)(6)
- 

To start the online meeting  
-----

1. Go to [\(b\)\(6\)](https://(b)(6))
2. If you are not logged in, log in to your account.





## Executive Summary

The HHS Cybersecurity Operations (CSO) maintains cyber security operational readiness and assurance that strengthens the security and resilience of HHS IT systems, networks, and critical infrastructure from cyber events and incidents. The HHS CSIRC Penetration Testing service within HHS CSO provides department-wide technical security controls assessment and testing capability by proactively identifying internal and external cyber and physical vulnerabilities. The HHS CSIRC Penetration Testing service has been tasked with reviewing third party security reports concerning findings for healthcare.gov and determining if HHS CSO concurs with the findings. The testing was performed using a combination of automated tools and manual review originating from an external non-attributable network. Due to time and access limitations the related findings are best effort. Below are proof of concepts authored by the HHS CSIRC Penetration Team as of February 4, 2014 showing vulnerabilities included in previous findings can be recreated:

Figure 1 shows a finding related to section 2.1.2 in the third party document titled "Healthcare gov Issues". In the original document, the author states healthcare.gov uses a Google Search Appliance and requests along with returned data are passed directly between healthcare.gov and the Google Search Appliance. HHS CSO discovered a URL under the healthcare.gov domain which has Google branding and appears to be a response directly from the Google Search Appliance.

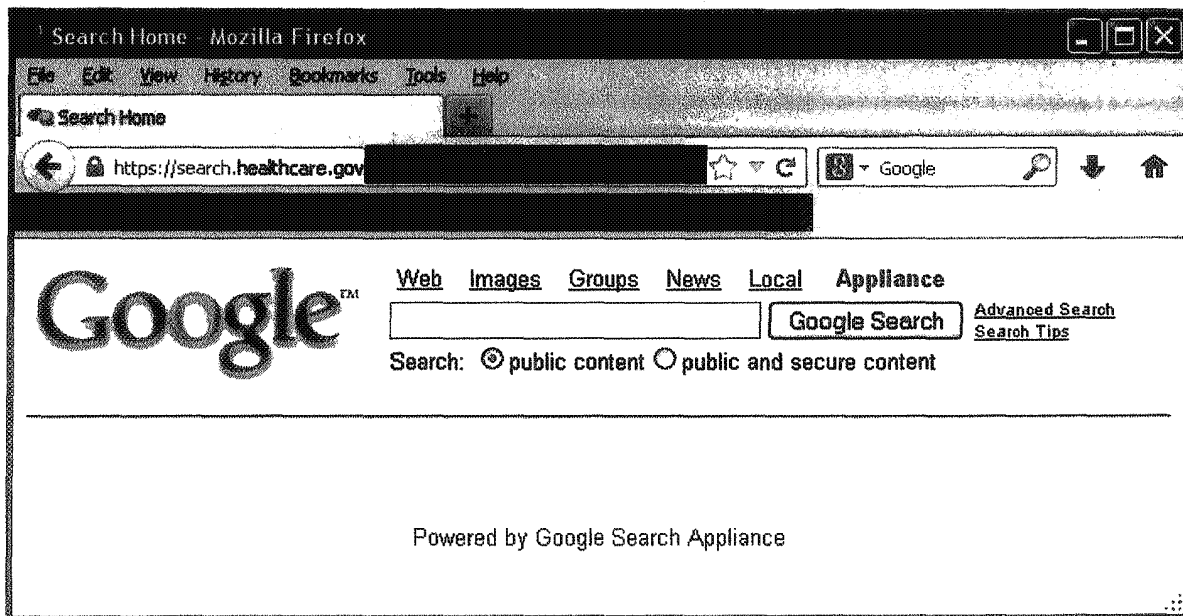


Figure 1: Google Branding on healthcare.gov site

Figure 2 shows a finding related to section 2.1.1 in the third party document titled "Healthcare gov Issues". In the original document, the author speculates that a vulnerability could be leveraged to inject fake search results on the healthcare.gov website. HHS CSO leveraged that information to provide a healthcare.gov URL which injects a fake search result and links to an arbitrary third party URL. Please note that the search result injection is not persistent; the only time the fake search result is present is when



the custom URL is used to access the site. However, a malicious actor could send a similar healthcare.gov URL to a victim to show arbitrary, fake results.

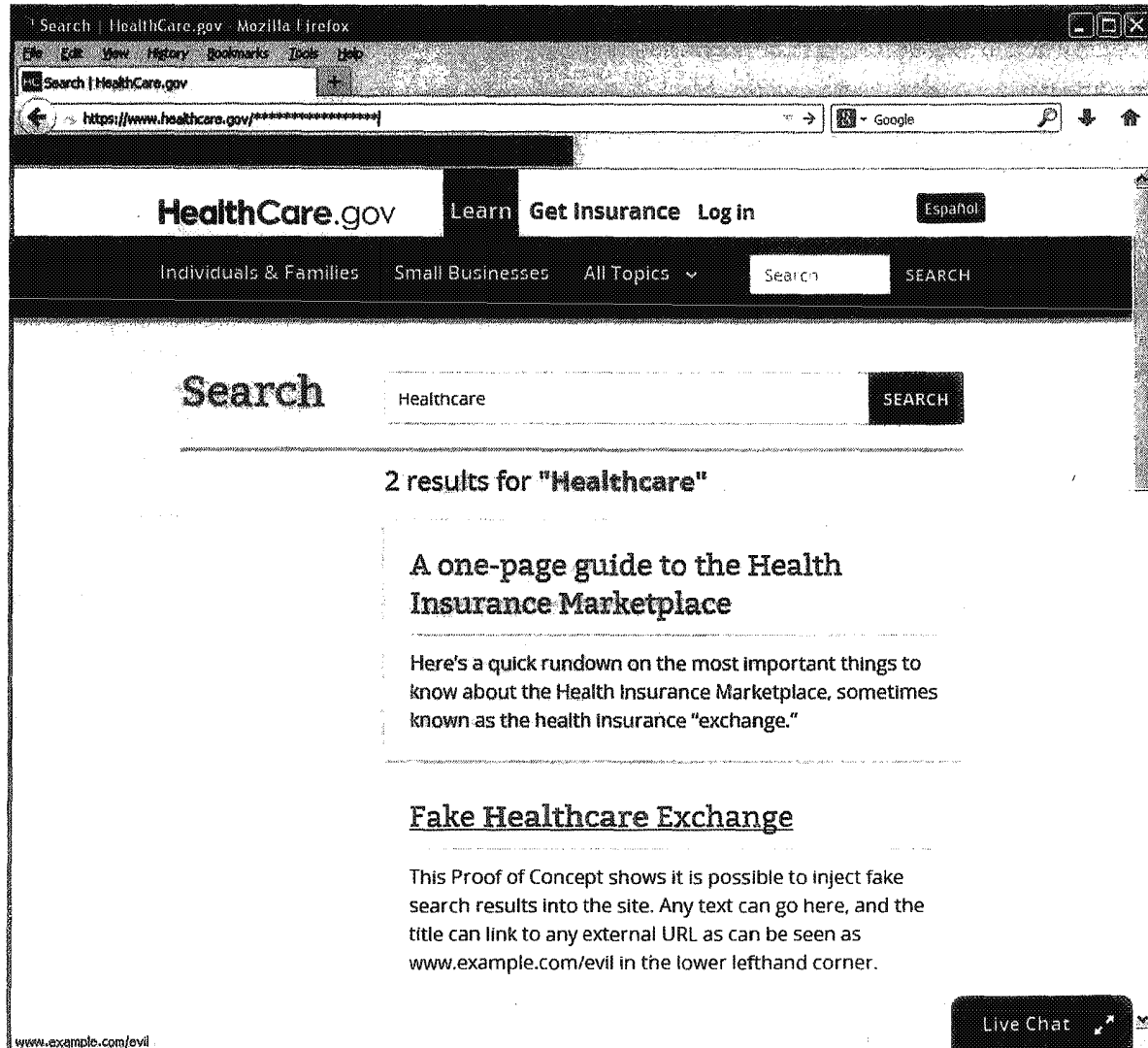
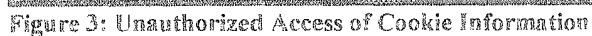


Figure 2: Fake Search Result

Figure 3 shows a finding related to section 2.5.2 in the third party document titled “Healthcare gov Issues”. In the original document, the author speculates vulnerabilities could be used to access cookie information. HHS CSO created this proof of concept to show how multiple vulnerabilities on healthcare.gov could be coupled together to provide unauthorized access to cookie information; the displayed text is the contents of the user’s cookie for the healthcare.gov site.





**Blank Page**

Appointment

**From:** Sivak, Bryan (HHS/IOS); [Redacted] **NotResp**  
[Redacted] **NotResp**  
**Sent:** 5/14/2013 4:17:53 PM  
**To:** Patel, Ketan (CMS/OC); [Redacted] **NotResp**;  
Herron, Julia (OS/IOS); [Redacted] **NotResp**  
[Redacted] **NotResp**; Booth, Jon G. (CMS/OC); [Redacted] **NotResp**  
[Redacted] **NotResp**  
**Subject:** HC.gov tech briefing  
**Location:** Bryan's office 614G  
**Start:** 5/16/2013 4:30:00 PM  
**End:** 5/16/2013 5:00:00 PM  
**Show Time As:** Busy  
**Recurrence:** (none)  
**Required Attendees:** Booth, Jon G. (CMS/OC); Herron, Julia (OS/IOS); Patel, Ketan (CMS/OC)

**When:** Thursday, May 16, 2013 12:30 PM-1:00 PM (GMT-05:00) Eastern Time (US & Canada).  
**Where:** Bryan's office 614G

**Note:** The GMT offset above does not reflect daylight saving time adjustments.

\*~\*~\*~\*~\*~\*~\*~\*~\*~\*

**From:** Herron, Julia (OS/IOS)  
**Sent:** Tuesday, May 14, 2013 11:49 AM  
**To:** Kendall, Damaris (HHS/OS)  
**Cc:** Sivak, Bryan (HHS/IOS)  
**Subject:** 30 mins for HC.gov tech briefing

Hi Damaris,

Jon Booth & Ketan Patel need to do a technical architecture briefing for Bryan sometime this week or next for the June launch of HC.gov – can you tell me when he has availability for a 30 minute time slot?

Thanks, Julie

Julia Herron  
Product Manager, Healthcare.gov  
U.S. Department of Health and Human Services (OS/IOS)  
Hubert H. Humphrey Building, Room 645F.12  
phone: 202-205-5127  
mobile: [Redacted] (b)(6)

**Blank Page**



Appointment

**From:** Herron, Julia (OS/IOS) NotResp  
NotResp

**Sent:** 2/15/2013 7:24:19 PM

**To:** Patel, Ketan (CMS/OC) NotResp  
'Andy Switky' [aswitky@ideo.com]; Slavinsky, Gary F. (CMS/OC) NotResp  
NotResp Trefzger, William (CMS/DWO) NotResp  
NotResp Edward Mullen'  
[ed@edmullen.com]; Kim, Richard K. (CMS/OC) NotResp  
NotResp Nethery, Charles F. (CMS/CTR) NotResp  
NotResp Burch,  
Mimi Z. (CMS/OC) NotResp Brice, Ebony  
M. (CMS/OC) NotResp  
NotResp Lupaeter, Melissa D. (CMS/OC) NotResp  
NotResp jessica@jjomedia.com; Perkins, Valerie (CMS/OC)  
NotResp; Robinson, Tamica (CMS/OC)  
NotResp  
NotResp; Le, Thao Q. (CMS/OC) NotResp  
NotResp Pressley, Erin L. (CMS/OC) NotResp  
NotResp Booth, Jon G. (CMS/OC) NotResp  
NotResp; Aviles, JuanCarlos (CMS/OC)  
NotResp  
NotResp Majmudar, Vidit S. (CMS/OC) NotResp  
NotResp Sivak,  
Bryan (HHS/IOS) NotResp  
NotResp Ramsey, Letticia T. (CMS/OC) NotResp  
NotResp; Carter, Daniel (CMS/OC) NotResp  
NotResp; Stoltz, Craig (HHS/ASPA) NotResp  
NotResp; Tudor, Susan J. (CMS/OC) NotResp  
NotResp Amos, Robert E. (CMS/OC)  
NotResp  
NotResp; Lartey, Aaron N. (CMS/OC) NotResp  
NotResp; Calabrese, Anthony (HHS/ASPA) NotResp  
NotResp  
Mark, William (CMS/OC) NotResp  
NotResp Mohs, Dean F. (CMS/CCIO) NotResp  
NotResp  
Jaworski, Jessica (CMS/OC)  
Garrard, Robert (CMS/OC)  
Mudd, Nathaniel (CMS/OC)  
Mitchell, Michael F.  
(CMS/OC) NotResp Lindenstruth,  
Gregory W. (CMS/OC) NotResp  
NotResp kevin.mcdermott@aquilent.com; Johnson, James E.  
(CMS/OC) NotResp  
NotResp

**CC:** 'Guthrie, Tamara' [tamara.guthrie@aquilent.com]; 'Cohen, Judy' [judy.cohen@aquilent.com]; 'Jeff Grieve'  
[jeff@jjomedia.com]; 'Joseph Busch' [jbusch@taxonomystategies.com]; 'Manambedu, Lakshmi (CGI Federal)'  
[Lakshmi.Manambedu@cgifederal.com]; Zerhusen, Eileen G. (CMS/OC) NotResp  
NotResp 'Warsaw, Craig' [Craig.Warsaw@aquilent.com]; 'Zeiders,  
Chris (CGI Federal)' [chris.zeiders@cgifederal.com]; 'Nethery, Charles' [charles.nethery@aquilent.com]; 'Gibb,  
Nathan' [Nathan.Gibb@aquilent.com]; Oh, Mark U. (CMS/OIS) NotResp



Obtained via FOIA by Judicial Watch, Inc.

NotResp [redacted] 'Ryan Co' [ryan@jjomedia.com]; 'Waple, Elisabeth (CGI Federal)' [Elisabeth.Waple@cgifederal.com]; 'Sheila Walsh' [SWalsh@palladianpartners.com]; Webber, JoAnn (CMS/OIS) [redacted] NotResp [redacted]

[redacted] NotResp [redacted] Ian Hung B. (CMS/OIS) [redacted] NotResp [redacted]

[redacted] NotResp [redacted] Giacomelli, Rebecca (CMS/OC) [redacted] NotResp [redacted]; Everette, Maria E. (CMS/OC) [redacted] NotResp [redacted]

[redacted] NotResp [redacted] Bonner, Mary (CMS/OC) [redacted] NotResp [redacted]

[redacted] NotResp [redacted] 'Weiss, Paul (CGI Federal)' [Paul.Weiss@cgifederal.com]; 'Hodges, Kim' [kim.hodges@aquilent.com]; St. Louis, Aileah (CMS/OC) [redacted] NotResp [redacted]

[redacted] NotResp [redacted] 'Vivian Bliss' [redacted] NotResp [redacted]

[redacted] NotResp [redacted] [vbliss@taxonomystrategies.com]

**Subject:** Healthcare.gov 2.0 Kickoff Meeting  
**Location:** Room B311 at 7111 Security Boulevard

**Start:** 2/20/2013 4:00:00 PM  
**End:** 2/20/2013 7:00:00 PM  
**Show Time As:** Busy

**Recurrence:** (none)

**Required Attendees:** Booth, Jon G. (CMS/OC); Patel, Ketan (CMS/OC); Trefzger, William (CMS/DWO); Mudd, Nathaniel (CMS/OC); 'Edward Mullen'; 'jessica@jjomedia.com'; Burch, Mimi Z. (CMS/OC); Amos, Robert E. (CMS/OC); Nethery, Charles F. (CMS/CTR); Stoltz, Craig (HHS/ASPA); Calabrese, Anthony (HHS/ASPA); Sivak, Bryan (HHS/IOS); Majmudar, Vidit S. (CMS/OC); Ramsey, Letticia T. (CMS/OC); Mitchell, Michael F. (CMS/OC); Robinson, Tamica (CMS/OC); Liupaeter, Melissa D. (CMS/OC); Johnson, James E. (CMS/OC); Tudor, Susan J. (CMS/OC); 'kevin.mcdermott@aquilent.com'; 'Andy Switky'; Lartey, Aaron N. (CMS/OC); Mark, William (CMS/OC); Carter, Daniel (CMS/OC); Brice, Ebony M. (CMS/OC); Pressley, Erin L. (CMS/OC); Slavinsky, Gary F. (CMS/OC); Lindenstruth, Gregory W. (CMS/OC); Jaworski, Jessica (CMS/OC); Garrard, Robert (CMS/OC); Le, Thao Q. (CMS/OC); Mohs, Dean F. (CMS/CCIIO); Aviles, JuanCarlos (CMS/OC); Kim, Richard K. (CMS/OC); Perkins, Valerie (CMS/OC)

PLEASE NOTE WE WILL BE IN ROOM B311 AT 7111 SECURITY BLVD (Behind Panera Bread as you come down Security Blvd heading to CMS Headquarters).

For those attendees conferencing in, we will send details in the morning. Thanks, Julie Herron

\*\*\*\*\*

Hello everyone,

As many of you are aware, we're in the process of ramping up front-end development efforts for Healthcare.gov 2.0 and want to formally kick-off the project this coming Wednesday, 2/20. Efforts are already underway and we have a great deal of work to be done to get us to the June 1<sup>st</sup> Redesign Launch and ultimately our October 1<sup>st</sup> Launch of the Marketplace features & functionality.

We will be providing an overview of the project goals and guiding principles, our development process, team introductions and next steps. It's going to be an action-packed agenda and we're looking to harness all the energy and excitement that has been circling around these efforts and focus it towards a successful implementation.

Room & VTC details for attendees from DC & other locales will be forthcoming. Our contracting partners will also be present for this meeting.

I'm looking forward to meeting everyone in person and seeing this project take shape in the coming weeks and months. In the meantime, if you have any questions, please contact me or Ketan Patel.

Julie Herron  
Product Manager, Healthcare.gov 2.0

# TESTING INSTRUCTIONS

## ENVIRONMENTS:

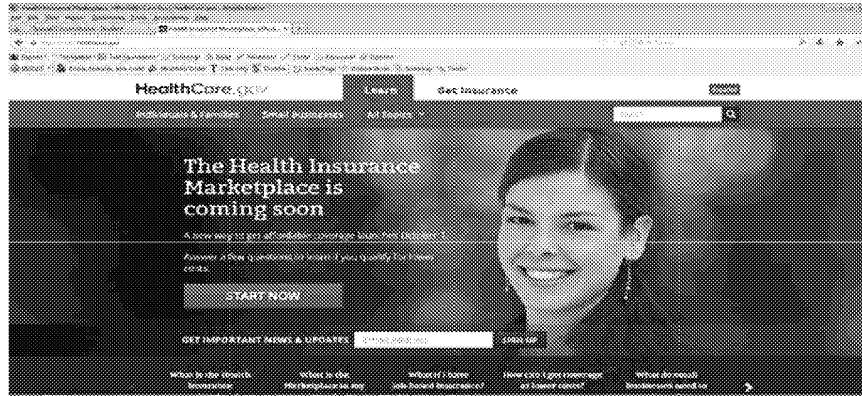
- TEST 

NotResp
- PROD PRIME

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.

# Steps to access FFM

- Go to <https://healthcare.gov/?ACA=> using Firefox or Chrome (IE has known issues and may have intermittent issues).
- You will arrive at this page:



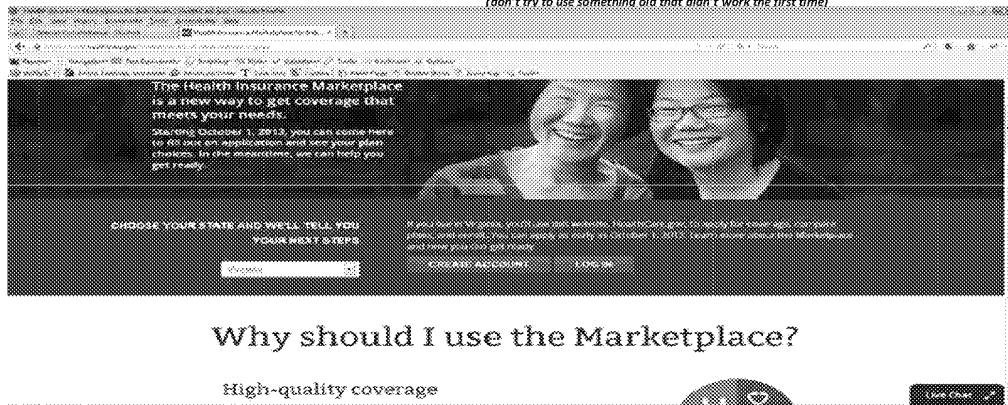
- Select 'Get Insurance tab' at the top right

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.

# FFM Steps Continued

- Select the state from the drop down
- Click either:
  - 'Create Account' button ( if you don't have profile) or
  - 'Login' (if you already have an account)

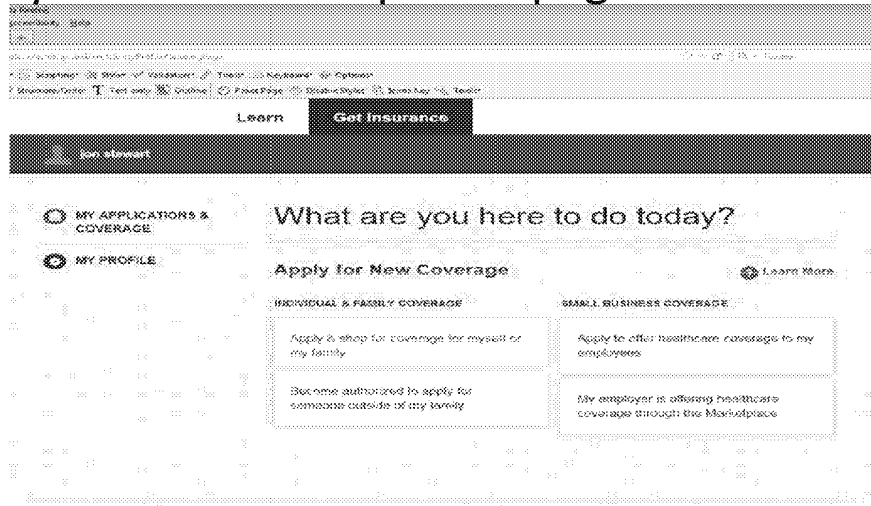
• *Note: Life Account functionality also has some issues from time to time. I would say – start from scratch creating an account, use absolutely new username and password, security questions, etc. (don't try to use something old that didn't work the first time)*



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.

# FFM Steps Continued

- After keying in valid credentials and logging in you will see the profile page



INFORMATION NOT RELEASED TO THE PUBLIC UNDER FOIA. This information may not be publicly disclosed and may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). This information 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.

- Verify the state abbreviation in your url matches the state you chose on the Get Insurance page prior to login/account creation (if i
- Choose ‘Apply and Shop for coverage for myself or my family’ link and begin the application



# Plan Compare

- Once you receive Eligibility Results open a new page for:

For Anonymous Shopper use:

- [https://\[NotResp\]healthcare.gov/Marketplace/DE/en\\_US/planCompare](https://[NotResp]healthcare.gov/Marketplace/DE/en_US/planCompare)
  - Please change the state according to the zip codes you use IF it doesn't show up correctly in the link
    - Landing on the Anonymous page > insert the zip code you would like to use
    - Proceed with testing

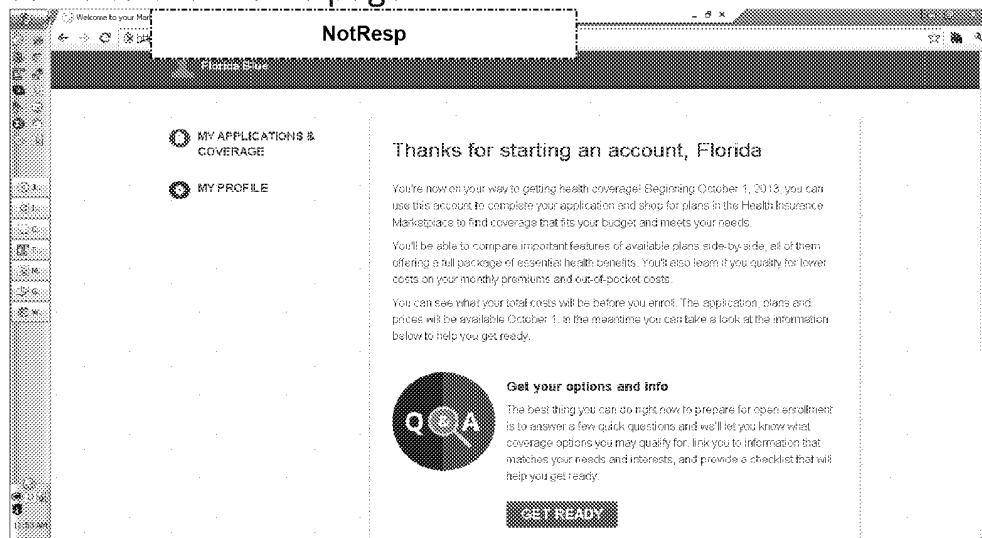
For non-Anonymous use:

- [https://\[NotResp\]healthcare.gov/Marketplace/auth/DE/en\\_US/planCompare](https://[NotResp]healthcare.gov/Marketplace/auth/DE/en_US/planCompare)
  - Please change the state according to the zip codes you use IF it doesn't show up correctly in the link
    - Insert respective App ID (twice)
    - Proceed with testing

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.

# Direct Enrollment

- Once you redirect to FFM from your website in **NotResp** you will come to the Profile page:



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.

## DE: Accessing the application

- Once you see this profile page, manually copy the url below into a new page to access the Individual application in NotResp

[https://NotResphealthcare.gov/marketplace/auth/VA/en\\_US/individualApplication](https://<span>NotResp</span>healthcare.gov/marketplace/auth/VA/en_US/individualApplication)

- The tenant ID/state abbreviation in the url needs to be replaced with the state you are applying in (i.e. SC)

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.

## DE: Eligibility Results

- Once you receive Eligibility Results scroll to the bottom of the results page and click the 'Redirect to Issuer Site' button
  - Verify correct redirection to your site for shopping
- Enroll in Plan and Submit

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.

# ACCESS to FFM in PROD PRIME ENVIRONMENT

- Prod Prime URL:

[https://NotResp.ms.gov/Marketplace/global/en\\_US/registration](https://NotResp.ms.gov/Marketplace/global/en_US/registration)

- Follow directions to create an account as stated in the above slides
- Login after creating account/existing credentials.
- Click on the 'apply&shop for coverage for myself or my family' link which will then redirect you to individual app.

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.

Message

**From:** Linares, George E. (CMS/OIS); [NotResp]  
[NotResp]  
**Sent:** 11/13/2013 4:14:20 PM  
**To:** Booth, Jon G. (CMS/OC); [NotResp]  
**CC:** Patel, Ketan (CMS/OC); [NotResp]  
Fryer, Teresa M. (CMS/OIS); [NotResp]  
[NotResp]; Marantan, James (CMS/OIS); [NotResp]  
[NotResp]; Horney, Mary P. (CMS/OIS); [NotResp]  
[NotResp]; Liggins, Leilani A. (CMS/OIS); [NotResp]  
[NotResp]  
Feuerberg, Lisa A. (CMS/OIS); [NotResp]  
**Subject:** RE: Healthcare.gov ATO  
**Flag:** Follow up

11:00 would work

Mary, Leilani, please set up a meeting for tomorrow with everyone on this distribution

Thanks

**George Linares**

*Acting Chief Technology Officer*

Centers for Medicare & Medicaid Services (CMS)

410.786.2866 [george.linares@cms.hhs.gov](mailto:george.linares@cms.hhs.gov)

7500 Security Blvd., N3-15-25

Baltimore, MD 21244-1850

Need more information? Visit [the OIS website](#).

**From:** Booth, Jon G. (CMS/OC)  
**Sent:** Wednesday, November 13, 2013 11:03 AM  
**To:** Linares, George E. (CMS/OIS)  
**Cc:** Patel, Ketan (CMS/OC); Fryer, Teresa M. (CMS/OIS); Marantan, James (CMS/OIS)  
**Subject:** Re: Healthcare.gov ATO

Sorry for the delay. Would tomorrow at either 11:00 AM or 1:00 PM work?

**From:** <Linares>, George Linares BB <[George.Linares@cms.hhs.gov](mailto:George.Linares@cms.hhs.gov)>  
**Date:** Wednesday, November 13, 2013 at 10:38 AM  
**To:** Jon Booth <[jon.booth@cms.hhs.gov](mailto:jon.booth@cms.hhs.gov)>  
**Cc:** Ketan Patel BB <[Ketan.Patel@cms.hhs.gov](mailto:Ketan.Patel@cms.hhs.gov)>, Teresa Fryer BB <[Teresa.Fryer@cms.hhs.gov](mailto:Teresa.Fryer@cms.hhs.gov)>, James Marantan BB <[James.Marantan@cms.hhs.gov](mailto:James.Marantan@cms.hhs.gov)>  
**Subject:** Re: Healthcare.gov ATO

Just wanted to follow up on these, please let's work on getting together this week.

CMS000696

Thanks

Sent from my iPad

On Nov 8, 2013, at 9:07 AM, "Booth, Jon G. (CMS/OC)" <[Jon.Booth@cms.hhs.gov](mailto:Jon.Booth@cms.hhs.gov)> wrote:  
George,

Thanks. We will send a system diagram and setup some time to talk next Tuesday if that will work for everyone. We are in agreement with this approach but we want to make sure we are all on the same page with defining which ECWS components constitute healthcare.gov and which don't.

Jon

**From:** <Linares>, George Linares BB <[George.Linares@cms.hhs.gov](mailto:George.Linares@cms.hhs.gov)>  
**Date:** Thursday, November 7, 2013 at 5:10 PM  
**To:** Jon Booth <[jon.booth@cms.hhs.gov](mailto:jon.booth@cms.hhs.gov)>, Ketan Patel BB <[Ketan.Patel@cms.hhs.gov](mailto:Ketan.Patel@cms.hhs.gov)>  
**Cc:** Teresa Fryer BB <[Teresa.Fryer@cms.hhs.gov](mailto:Teresa.Fryer@cms.hhs.gov)>, James Marantan BB <[James.Marantan@cms.hhs.gov](mailto:James.Marantan@cms.hhs.gov)>  
**Subject:** RE: Healthcare.gov ATO

Jon,

In consultation with the CISO, we think the best approach would be to do the following:

- Since Mitre still has funds, complete the SCA testing for just Healthcare.gov with the goal to secure an ATO — Mitre just needs a date to get started
- For the remainder of ECWS, develop a mitigation plan that outlines the steps and timelines for the other components of ECWS, including the migration to the VDC

These actions would cover ECWS from a security perspective and also will give you some flexibility in case the VDC move gets pushed back for whatever reason.

For the EZ App, I would recommend also engaging Monique and Kirk. If everyone agrees that this should be part of FFM, and then it should definitely be part of the FFM SCA in December. Probably having a quick meeting would be good, I know is difficult to go back and forth via email.

Thanks

**George Linares**

*Acting Chief Technology Officer*

Centers for Medicare & Medicaid Services (CMS)

<image001.jpg> 410.786.2866 <image002.jpg> [george.linares@cms.hhs.gov](mailto:george.linares@cms.hhs.gov)

7500 Security Blvd., N3-15-25

Baltimore, MD 21244-1850

Need more information? Visit [the OIS website](#).

**From:** Booth, Jon G. (CMS/OC)  
**Sent:** Thursday, November 07, 2013 2:00 PM  
**To:** Linares, George E. (CMS/OIS); Patel, Ketan (CMS/OC)  
**Cc:** Fryer, Teresa M. (CMS/OIS); Marantan, James (CMS/OIS)  
**Subject:** Re: Healthcare.gov ATO

George,

Thanks for flagging this. We are anxious to finish this up as well. I wanted to flag a couple of items and get your take on how this impacts scheduling the remaining activities.

Over the past 2 weeks, we have been working with the HP VDC team to discuss a migration of the ECWS systems from Terremark to the VDC. We are in the mix as one of the pilot systems to be migrated first. Given this, we are thinking it might make the most sense to get this migration complete and then re-audit in the new VDC environment. We are thinking this migration will occur around the end of the year.

Regarding the EZ app project that we are discussing on a separate thread, Mark Oh, Ketan and I have been discussing and we all agree that system more properly fits under the FFM family of systems. Our understanding is that there are upcoming audit activities for the FFM scheduled in mid-December and we'd recommend that the EZ app be looped into those activities.

Please let me know if we should grab some time to discuss these items further.

Jon

**From:** <Linares>, George Linares BB <[George.Linares@cms.hhs.gov](mailto:George.Linares@cms.hhs.gov)>

**Date:** Wednesday, November 6, 2013 at 10:32 AM

**To:** Ketan Patel BB <[Ketan.Patel@cms.hhs.gov](mailto:Ketan.Patel@cms.hhs.gov)>, Jon Booth <[jon.booth@cms.hhs.gov](mailto:jon.booth@cms.hhs.gov)>

**Cc:** Teresa Fryer BB <[Teresa.Fryer@cms.hhs.gov](mailto:Teresa.Fryer@cms.hhs.gov)>, James Marantan BB <[James.Marantan@cms.hhs.gov](mailto:James.Marantan@cms.hhs.gov)>

**Subject:** [Healthcare.gov](http://Healthcare.gov) ATO

Ketan and Jon,

The FO has been informed that currently [Healthcare.gov](http://Healthcare.gov) as part of Exchange Consumer Web Site (ECWS) FISMA system is operating without an ATO. EISG has asked MITRE to finalize the SCA report (of which no testing was done) due to not having an environment ready for testing (by end of August) and as well as being unable to get an alternate date for when the environment would be ready to complete the SCA activities. Operating without an ATO is a serious issue and it represents a high risk to the agency. OC needs to work with EISG to bring [Healthcare.gov](http://Healthcare.gov) under compliance. Please advise.

Thanks

**George Linares**

*Acting Chief Technology Officer*

Centers for Medicare & Medicaid Services (CMS)

<image001.jpg> 410.786.2866 <image002.jpg> [george.linares@cms.hhs.gov](mailto:george.linares@cms.hhs.gov)

7500 Security Blvd., N3-15-25

Baltimore, MD 21244-1850

Need more information? Visit [the OIS website](http://the.OIS.website).

<image001.jpg>

<image002.jpg>



Appointment

**From:** Bailey, Ayanna C. (CMS/OIS) NotResp

**Sent:** 10/24/2013 3:57:10 PM

**To:** Bailey, Ayanna C. (CMS/OIS) NotResp

NotResp; Van, Hung B. (CMS/OIS) NotResp

NotResp; James, Brian M. (CMS/CCIIO)

NotResp; Shropshire, Richard

NotResp

NotResp Tibbits, Paul A. (CMS/CCIIO) NotResp

NotResp; Redden, Corey L. (CMS/OIS) NotResp

NotResp; Underwood, Damon L.

(CMS/OIS) NotResp

NotResp; Radcliffe, Glenn D. (CMS/OIS) NotResp

NotResp Patel,

Ketan (CMS/OC) NotResp

Holliday, Jeff (CMS/OIS) NotResp

NotResp Reinhold, Billie (IHS/PHX) NotResp

NotResp Booth, Jon

G. (CMS/OC) NotResp; Reinhold,

Michael R. (CMS/OEM) NotResp

NotResp; Margush, Doug C. (CMS/OIS) NotResp

NotResp; Kohlway, David (david.kohlway@hp.com)

[david.kohlway@hp.com]; Kevin.cuellar@cgifederal.com; david.a.offenkrantz@hp.com; Williams, Brandon J.

(CMS/CIISG) NotResp

NotResp Kuhn, Jerry C. (CMS/OIS)

NotResp

Brandenburg, Heather (heather.d.brandenburg@hp.com) [heather.d.brandenburg@hp.com];

musharaf.rashid@cgifederal.com

**CC:** Royal, Letitia (CMS/OIS) NotResp

Plaugher, Mark J. (CMS/OIS) NotResp

NotResp; Mundy, Gordon D. (CMS/OIS) NotResp

NotResp; Lindenstruth, Gregory W.

(CMS/OC) NotResp

Maxwell, Aquila (CMS/OEM) NotResp

'White, Richard (CGI Federal)' [rick.white@cgifederal.com]; Flaherty, Leslie W. (CMS/OEM) NotResp

NotResp; 'Greg Fairnak' (greg@hcmdm.com)

[greg@hcmdm.com]; Fairnak, Gregory (CMS/CTR) NotResp

NotResp Russell, Christopher A. (CMS/OIS) NotResp

NotResp

**Subject:** Application Discovery Kick-Off Meeting

**Location:** C-115

**Start:** 10/31/2013 7:00:00 PM

**End:** 10/31/2013 8:00:00 PM

**Show Time As:** Busy

**Recurrence:** (none)

**Required** Van, Hung B. (CMS/OIS); James, Brian M. (CMS/CCIIO); Shropshire, Richard (CMS/CCIIO); Tibbits, Paul A.

**Attendees:** (CMS/CCIO); Redden, Corey L. (CMS/OIS); Underwood, Damon L. (CMS/OIS); Radcliffe, Glenn D. (CMS/OIS); Patel, Ketan (CMS/OC); Holliday, Jeff (CMS/OIS); Reinhold, Billie (IHS/PHX); Booth, Jon G. (CMS/OC); Reinhold, Michael R. (CMS/OEM); Margush, Doug C. (CMS/OIS); Kohlway, David (david.kohlway@hp.com); Kevin.cuellar@cgifederal.com; david.a.offenkrantz@hp.com; Williams, Brandon J. (CMS/CIISG); Kuhn, Jerry C. (CMS/OIS); Brandenburg, Heather (heather.d.brandenburg@hp.com); musharaf.rashid@cgifederal.com

VDC Application Discovery Kickoff 20131030 v3.pptx

Attached are the slides for today's meeting.

Hello,

This meeting is being scheduled to allow HP the opportunity to reach out to the system owners for the Health Insurance Marketplace (HIM) applications slated to transition from Terremark to HP's Tulsa Data Center. The purpose of the Application Discovery Process is primarily to allow HP the opportunity to determine any interdependencies and application specific requirements from the system owner perspective and begin collaborating with one another by having additional technical deeper-dive sessions on a smaller scale later to ensure that this transition is seamless for all parties involved.

An agenda will be attached by the early part of next week.

For remote participants a webinar and teleconference has been created for this discussion as well.

Thank you.

#### Webinar Information

[https://\(b\)\(6\).cms.hhs.gov/\(b\)\(6\)/](https://(b)(6).cms.hhs.gov/(b)(6)/)

Ayanna Bailey invites you to an online meeting using WebEx.

Meeting Number: (b)(6)

Meeting Password: This meeting does not require a password.

---

#### Audio conference information

---

1. Please call the following number:

WebEx: (b)(6)

2. Follow the instructions you hear on the phone.

Your WebEx Meeting Number: (b)(6)

---

To join from the Baltimore, Chicago, or Kansas City offices

-----  
1. Dial ext

(b)(6)

2. Enter the Meeting Number

(b)(6)

-----  
To join this meeting online

-----  
1. Go to [https://cms](https://cms.com/cms/j.php?J)

(b)(6)

com/cms/j.php?J

(b)(6)

2. If requested, enter your name and email address.

3. If a password is required, enter the meeting password: This meeting does not require a password.

4. Click "Join".

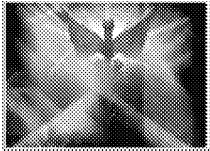
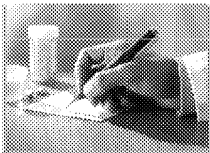
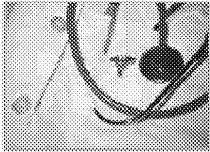
5. Follow the instructions that appear on your screen.



Centers for Medicare & Medicaid Services



## Virtual Data Center Health Insurance Marketplace



**VDC HIM Application Discovery Kick Off**  
**October 31<sup>st</sup>, 2013**

# Agenda

- Introductions
- Meeting Purpose / Scope / VDC Overview
- Key Application Discovery Focus Areas
- Transition Approach
- Technical Solution
- Next Steps
- Questions and Open Discussion



2

Slide Instructions:

[Insert Business Need, Goals/Scope/Purpose, and Stakeholders from the project's PSR Presentation. If PSR Presentation is not available, follow guidance provided in each section below.]

## High Level Project Scope & VDC Overview

- HP and CGI have been contracted to establish the VDC HIM Production Virtual Data Center (P VDC)  and Disaster Recovery Virtual Data Center (DR VDC)
- These two data centers must operate securely and reliably 24x7, 365 days a year. In the event of a disaster, DR-VDC HIM must provide production recovery.

# Risk and Mitigation

## *Minimizing risk through communication*

### **Risk**

- VDC HIM will not be able to fully manage the standup and operations support of the Exchange systems without proper knowledge transfer

### **Mitigation**

- Weekly "Scrum like" cycles with defined deliverables/goals like "Migration Plan for HIOS" and to identify backlog items and work elements.
- Pairing of VDC resources within project teams to supplement KT sessions by incrementally learning critical details of current build and deploy processes, dependencies etc.
- Continuous monitoring through weekly cycles to identify High Risk High Value items to enable backlog prioritization and risk mitigation.

# Application Discovery

*For IMPL & Prod Environments*

## Focus Areas

- Release / Deploy
- Operations Support

## Key Outcomes

1. Establish Working Group Sessions
2. Certify Application Prioritization
3. Specific Key Documentation
  1. System Architecture Diagrams
  2. Operations and Maintenance Manuals
  3. Release / Deploy Process Manuals
  4. Test Plan & Scripts



### Slide Instructions:

[Provide a summary of the test case results obtained for the reported test effort from Table 2 of the Test Summary Report.



# HIM System Logical Groups

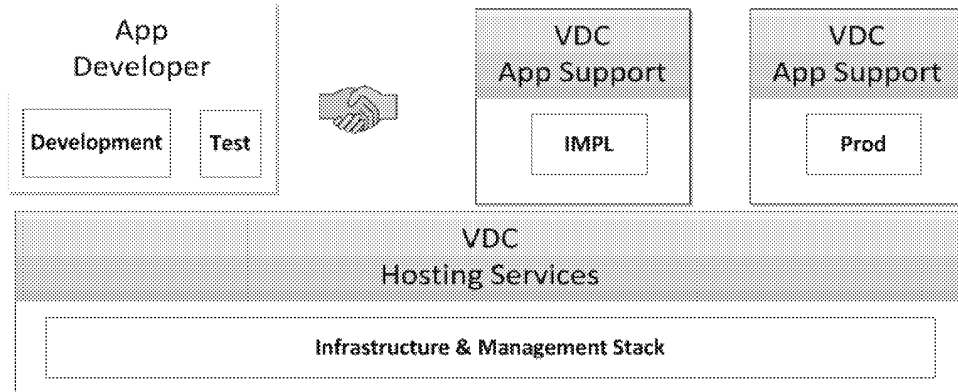
## System Interdependencies / Initial Grouping

Non FEPS Systems	FEPS Systems	Other Infrastructure & Third Party Software
SERTS/SERVIS	FFM	CMSNet (MPLS)
VAMS	DSH	<b>NotR</b> Work Scheduler
CPMS	MIDAS	<b>NotResp</b> Ops Manager)
CALT	HIOS + (finder.healthcare.gov)	ECWS (Akamai Content Delivery)
zONE	HIAD	
CMMI	RBIS	
	EIDM	
	TEFT	
	<b>NotResp</b>	
	SAS	

### Slide Instructions:

[Provide a summary of the test incidents that were reported during the testing from Table 3 of the Test Summary Report, which is included below:]

## VDC Support Model

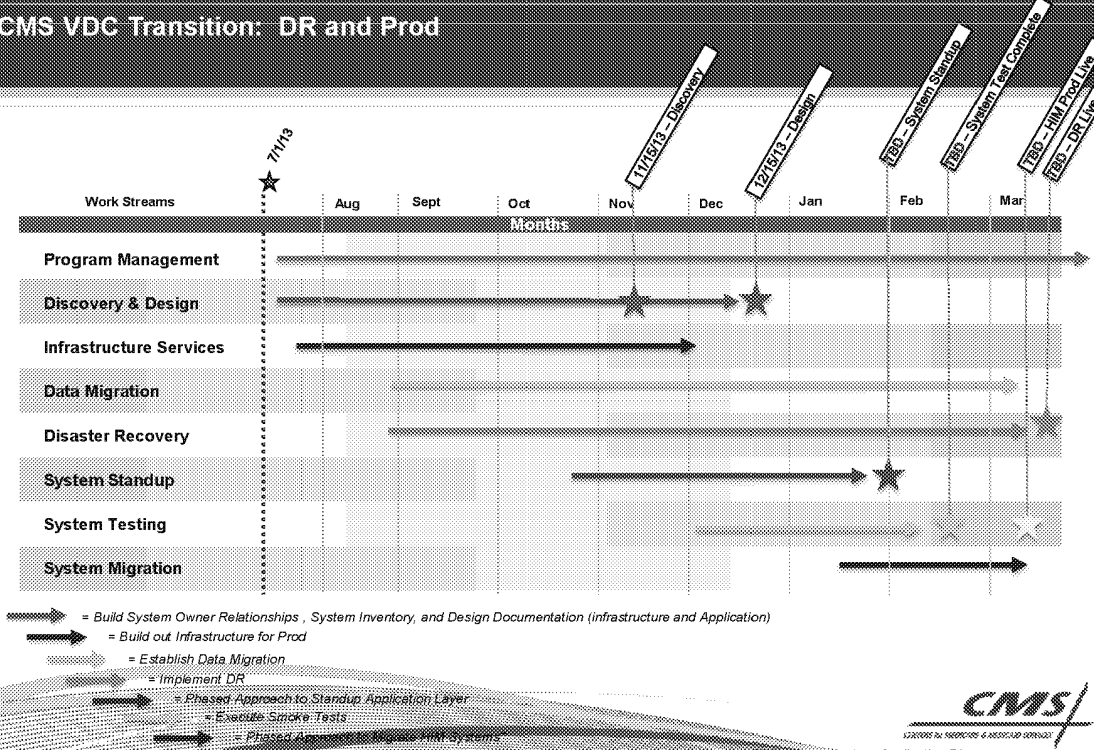


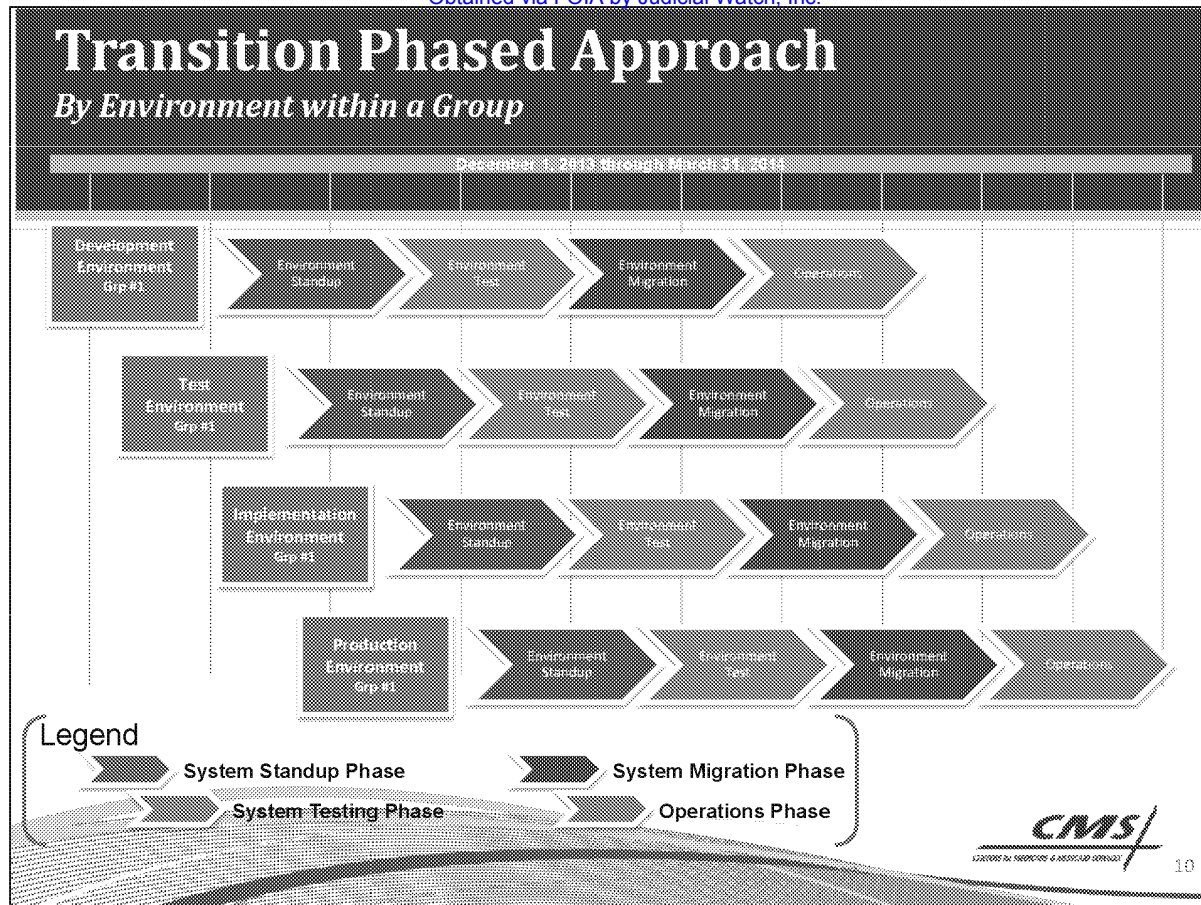
# Transition Approach



# Transition Timeline

## CMS VDC Transition: DR and Prod





**Slide Instructions:**

[Using the table shown on this slide, provide the Performance Goals and Measures that will be used to assess the degree of success for this project. The Measurement Area, Measurement Category and Measurement Indicator should be based upon the Federal Enterprise Architecture (FEA) Performance Reference Model (PRM), more information for which can be found within the FEA Consolidated Reference Model (CRM) document located on the OMB website.]

# Technical Solution

# Four Step Process for each environment Standup

## Physical Environment Build out

- Network
- Base Virtual Machine
- Baseline OS with management utilities
- Integrate with Management stack

NotResp

## Data Migration

- Snap mirror replication to array
- Mount clone (virtuix) data files from Terremark onto HP VMs
- Localize images to HP environment
- Setup VDC system administrators

NotResp

NotResp

## Verification of Application Platforms, Integration

- Verify application platform configurations
- Validate environment stovepipe integration
- Validate Load Balancers

Bring up the environment in parallel to Terremark environment

**CMS/**  
SOLUTIONS IN TELECOM & ASSOCIATED SERVICES



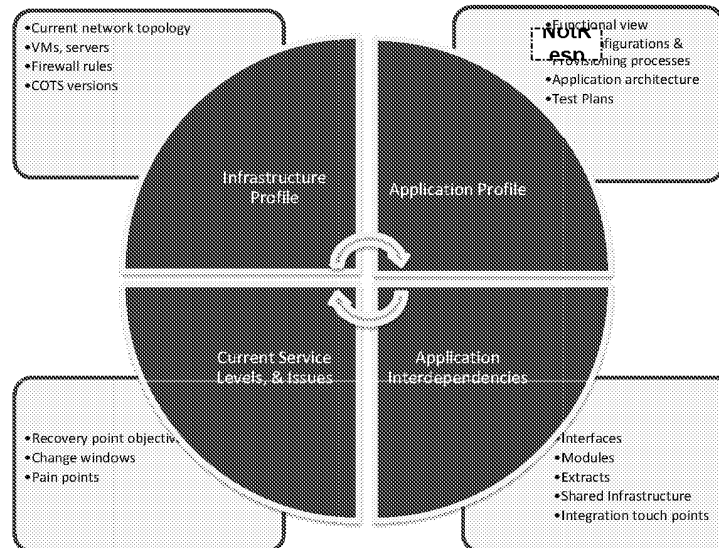
# VDC HIM Environment Standup

## *Key Discovery Output*

- Architecture Diagrams
- Knowledge of the system (i.e., Modules of FFM)
- Interfaces & Interdependencies
- Technical configurations (e.g. NotResp Web Services)
- Validation procedures
- Key contacts (e.g., System Architect, Sr. DBA)

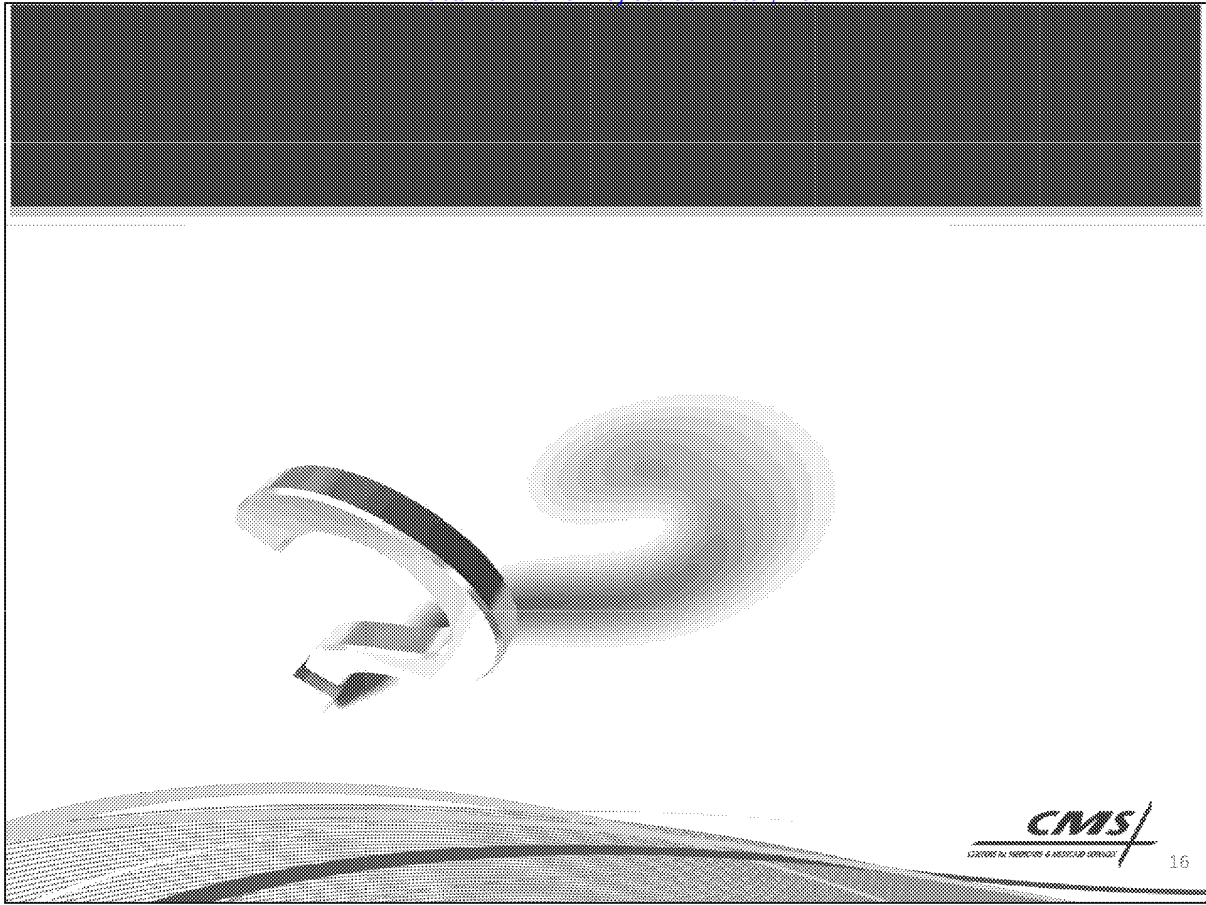
# Application & Infrastructure Discovery

*Bundle of Key Information per Application*



## Next Steps

- Identify groups for detailed working sessions
- Establish working session dates
- Specific Key Documentation
  - System Architecture Diagrams
  - Operations and Maintenance Manuals
  - Release / Deploy Process Manuals
  - Test Plan & Scripts



## Appointment

**From:** Yelena Buchynsky [ybuchynsky@qssinc.com]**Sent:** 5/16/2014 4:29:43 PM

**To:** Karlton Kim [kkim@qssinc.com]; Oh, Mark U. (CMS/OIS); [NotResp]; [NotResp]; Chao, Henry (CMS/OIS); [NotResp]; [NotResp]; Fender, Rebecca (CMS/OIS); [NotResp]; [NotResp]; scott.gilliland@accenturefederal.com; Walter, Stephen J. (CMS/OIS); [NotResp]; [NotResp]; Richardson, Marc D. (CMS/OIS); [NotResp]; [NotResp]; Basavaraju, Venkat (CMS/OIS); [NotResp]; [NotResp]; Patel, Ketan (CMS/OC); [NotResp]; [NotResp]; Booth, Jon G. (CMS/OC); [NotResp]; [NotResp]; Sharad Baranwal [sbaranwal@qssinc.com]; Manik Naik [mnaik@qssinc.com]; Raj Doraiswamy [rdoraiswamy@qssinc.com]; Dmitry Shkolnik [dshkolnik@qssinc.com]; Kovilvenni Ramaswamy [kramaswamy@qssinc.com]; Frederick Wilke [fwilke@qssinc.com]; 'Scott Gilliland' [scott.gilliland@accenture.com]; John Ward [john.ward@optum.com]; 'greta.peterson@optum.com' [greta.peterson@optum.com]; Reilly, Megan C. (CMS/OC); [NotResp]; [NotResp]; Custer, Edward (CMS/OIS); [NotResp]; [NotResp]; Falk, Paige E. (CMS/OIS); [NotResp]; [NotResp]; Kothapalli, Jeevan (CMS/OIS); [NotResp]; [NotResp]; Giacomelli, Rebecca (CMS/OC); [NotResp]; [NotResp]; 'hilda.lu@accenturefederal.com' [hilda.lu@accenturefederal.com]; Constance Kahler [ckahler@qssinc.com]; scott.a.wilcox@accenturefederal.com; Eric Ritter [eritter@qssinc.com]; Vijay Hiregoudar [vhiregoudar@qssinc.com]; Mansaray, Sharlene (CMS/OIS); [NotResp]; [NotResp]; Andy Alasso [andy.alasso@optum.com]; Kane, David (CMS/OIS); [NotResp]; daniel.gralewski@oracle.com; dinesh.k.jayapalan@accenturefederal.com; raja.a.thangavelu@accenturefederal.com; Yelena Buchynsky [ybuchynsky@qssinc.com]

**CC:** Carter, Cathy T. (CMS/OIS); [NotResp]; [NotResp]; 'stephen.wass@accenturefederal.com' [stephen.wass@accenturefederal.com]; 'amy.s.park@accenture.com' [amy.s.park@accenture.com]; 'paulo.villela@accenture.com' [paulo.villela@accenture.com]; Junni Rajbhandari [jrajbhandari@qssinc.com]; Nitin Matta [nmatta@qssinc.com]; Girish Shetty [gshetty@qssinc.com]; Krishnamoorthi Ganesan [kganesan@qssinc.com]; Vignesh Srinivasan [vsrinivasan@qssinc.com]; Jacob, Baiju [baiju.jacob@optum.com]

**Subject:** SLS Integration**Location:** Presentation Room A COL3 - 12th Floor; WebEx and Dial-in instructions (for those who will not be attending in-person) below**Start:** 5/16/2014 5:30:00 PM**End:** 5/16/2014 8:00:00 PM**Show Time As:** Busy**Recurrence:** (none)**Required** Karlton Kim; Oh, Mark U. (CMS/OIS); Chao, Henry (CMS/OIS); Fender, Rebecca (CMS/OIS);**Attendees:** scott.gilliland@accenturefederal.com; Walter, Stephen J. (CMS/OIS); Richardson, Marc D. (CMS/OIS); Basavaraju, Venkat (CMS/OIS); Patel, Ketan (CMS/OC); Booth, Jon G. (CMS/OC); Sharad Baranwal; Manik Naik; Raj Doraiswamy; Dmitry Shkolnik; Kovilvenni Ramaswamy; Frederick Wilke; 'Scott Gilliland'; John Ward; 'greta.peterson@optum.com'; Reilly, Megan C. (CMS/OC); Custer, Edward (CMS/OIS); Falk, Paige E. (CMS/OIS); Kothapalli, Jeevan (CMS/OIS);

Giacomelli, Rebecca (CMS/OC); 'hilda.lu@accenturefederal.com'; Constance Kahler;  
scott.a.wilcox@accenturefederal.com; Eric Ritter; Vijay Hiregoudar; Mansaray, Sharlene (CMS/OIS); Andy Alasso;  
Kane, David (CMS/OIS); daniel.gralewski@oracle.com; dinesh.k.jayapalan@accenturefederal.com;  
raja.a.thangavelu@accenturefederal.com

Updated slides attached. Added an "Integration" section to add more details on specific integration points.

---

Hello,

You are invited to participate in SLS Integration review this Friday at 1:30 PM.

This meeting will take place in our Columbia 3 location on the 12<sup>th</sup> floor in our Presentation Room (10480 Little Patuxent Parkway, Suite 1200, Columbia, MD 21044).

Columbia 3, 12<sup>th</sup> floor is a secure area, so you will need to be escorted to your meeting. Upon arrival proceed to the 11<sup>th</sup> floor (this floor has an open access) and stop at the receptionist desk (left from the elevator) to sign-in and receive a temporary badge. Receptionist will escort you to the 12<sup>th</sup> floor. *Please allow extra time for sign-in procedure.*

---

#### Meeting Agenda:

1. Overview and purpose of SLS
2. Refresh on scope of SLS (i.e. consumer accounts)
3. General framework for what it will handle
4. Quick review of what's in & out
5. High Level Design Discussion
6. Order of steps towards implementation
7. Migration plans and timing (i.e. EIDM migration path, RIDP & FFM integrations)
8. Implementation Approach and Timeframes
9. Develop a system integration inventory and points of contact
10. Develop a key decisions inventory and owner(s)
11. Develop a required clearances inventory and owner(s)
12. High level timeline including major milestones and migration points
13. Next Steps

#### Materials:

---

WebEx and Dial-in for those who will not be attending in-person.

---

#### Meeting Information

Topic: SLS Integration

Date: Friday, May 16, 2014

Time: 1:30 pm, Eastern Daylight Time (New York, GMT-04:00)

Meeting Number: (b)(6)

Meeting Password: (b)(6)

To start or join the online meeting

Go to [\(b\)\(6\)](https://(b)(6))

Audio conference information

US TOLL (b)(6)  
Access code (b)(6)

(let me know if you cannot use US TOLL number)

Thank you,

***Yelena Buchynsky*** | QSSI | [www.qssinc.com](http://www.qssinc.com)

10480 Little Patuxent Parkway, Suite 1200, Columbia, MD 21044

Work: 301.977.7884 Ext. 757

Cell: (b)(6)

[ybuchynsky@qssinc.com](mailto:ybuchynsky@qssinc.com)



**CMMI® Maturity Level 3 Rated**

**GSA Approved HSPD-12 System Integrator**



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.



# Scalable Login System

# Purpose

Improve healthcare.gov reliability with Scalable Login System (SLS), a web-scale consumer user account system.

# Overview

- Implement login and EIDM Web Services interface using MPL's scalable architecture.
- No FFM refactoring needed from Accenture.
- Configuration change / minor patches only.
- Inherit the security and scalability controls which have been fully audited on MPL.
- Provide existing customer support functions.

# **User experience stays the same**

- **Seamless data migration for existing consumer users.**
- **Non-consumer users continue to use EIDM.**



# Minimal FFM impact

- Update EIDM web services endpoint URL.
- Recognize SLS NotResp assertion.

# High Level Design

healthcare.gov  
Scalable Login System (SLS)  
Architecture Overview  
Author: james@hcgov.us  
Revision: 2014-05-15

NotResp

healthcare.gov  
SLS login dataflow  
Authors: james@hgov.us, joey@hgov.us  
Revision: 2014-05-15

NotResp



# Integration

# FFM

- Update EIDM web services endpoint URL.
- Recognize SLS

NotResp

assertion.

# EIDM

- One-time migration of consumer user accounts.
- No ongoing integration.

# RIDP

- SLS will connect to RIDP service either directly (as EIDM does currently) or via Data Services Hub.
- Currently evaluating both options.



# SERCO

- SLs will provide an interface to find a user and upgrade to loa2.
- Will replace NotResp console, which exposes too much functionality (can edit all fields for all users) and has taken down healthcare.gov multiple times (because of expensive find user queries).

# NGD / Call Centers

- NGD uses FFM web services, for example, to reset a user's password.
- Since FFM will use SLS's EIDM web services endpoint, no further integration necessary to support NGD.

# SHOP

- SLS will not support SHOP users.
- SHOP users will use EIDM.



# Reporting

- SLS will provide queries for analytics of user behavior patterns.
- These queries will run on a replicated, non-production-traffic DB instance.
- Complete audit logs will be kept of all administrative functions (search, modify user, etc.).



# XOC / Ops

- SLS will use NotResp for performance monitoring.
- SLS will work with XOC to develop operations playbook, escalation procedures, on-call pager rotation, etc.

# Disaster Recovery

- No additional work needed. SLS inherits DR strategy of Application 2.0.
- AWS uses isolated regions and availability zones for maximum stability and fault tolerance.
- Master slave replication and automated backups for DB fault tolerance.

# Loadtesting

- Will loadtest specific operations and patterns of user behavior (for example: all the steps needed to create an account, loa1, loa2).
- Need EIDM loadtesting results in order to establish baseline and make apples-to-apples comparisons.

# Next Steps



# Account migration testing




- Need access to dev environment user account data from [REDACTED] in order to test migrations into SLS.
- Working with Venkat, Rebecca on a Data Migration Plan to proceed with access.

NotResp

# RIDP testing

- SLS needs to connect to RIDP service to implement EIDM web services.
- Can connect to RIDP service directly or via DSH.
- Need test access to DSH to test connecting to RIDP via DSH.

# SAML assertion

- FFM verifies  validity by checking its signature.
- SLS can either:
  1. Sign  just like EIDM. Need EIDM cert.
  2. Sign  with new signature. Need FFM to recognize new SLS signature.



# **EIDM web services testing**

- QSSI has developed a comprehensive test suite for EIDM web services.
- Should use the same test suite to test SLS's implementation of EIDM web services.
- SLS team has outdated and/or misconfigured version of test suite.
- Need to get working test suite.



Appointment

**From:** Wallace, Mary H. (CMS/OC) NotResp

**To:** NotResp

Bataille, Julie (CMS/OC) NotResp

NotResp Reilly, Megan C. (CMS/OC) NotResp

NotResp]; Liverpool, Sheila Faison (CMS/OC)

NotResp

NotResp Broccolino, Michele (CMS/OC) NotResp

NotResp Booth, Jon G. (CMS/OC) NotResp

NotResp]; St. Louis, Aileah (CMS/OC) NotResp

NotResp Trefzger, William (CMS/DWO) NotResp

NotResp

Patel, Ketan (CMS/OC) NotResp

Harris, Danielle Y. (CMS/OC) NotResp

NotResp Mitchell, Michael F. (CMS/OC) NotResp

NotResp Ramsey, Letticia T. (CMS/OC) NotResp

NotResp Iacomelli, Rebecca (CMS/OC) NotResp

NotResp]; Pressley, Erin L. (CMS/OC) NotResp

NotResp]; Miner, Amy L. (CMS/OC)

NotResp Stoltz, Craig (CMS/OC)

NotResp

NotResp Das, Krista (CMS/OC) NotResp

NotResp Franklin,

Julie G. (CMS/OC) NotResp

Harmatuk, Frances R. (CMS/OC) NotResp

NotResp Johnson, Naomi E. (CMS/OC) NotResp

NotResp Carey, Kathleen G. (CMS/OC) NotResp

NotResp

Broccolino, Mark D. (CMS/OC) NotResp

NotResp Burdette, Jeffrey (CMS/OC) NotResp

NotResp Tudor, Susan J. (CMS/OC) NotResp

NotResp CMS VTC NotResp

NotResp Wallace, Mary H. (CMS/OC) NotResp

NotResp

**CC:** English, Letitia N. (CMS/OC) NotResp

NotResp Hollman, Susan K. (CMS/OC) NotResp

NotResp Bogley, Dennis (CMS/OC) NotResp

NotResp Panicker, Anita G. (CMS/OC)

NotResp Johnson, James E.

(CMS/OC) NotResp

NotResp Burch, Mimi Z. (CMS/OC)

NotResp

**Subject:** Weekly Marketplace Consumer Tools Meeting

**Location:** OC Conference Room S1-20-01 (Baltimore) / 303D04 (DC) / Call In (b)(6) Meeting (b)(6)

**Start:** 5/21/2014 4:30:00 PM

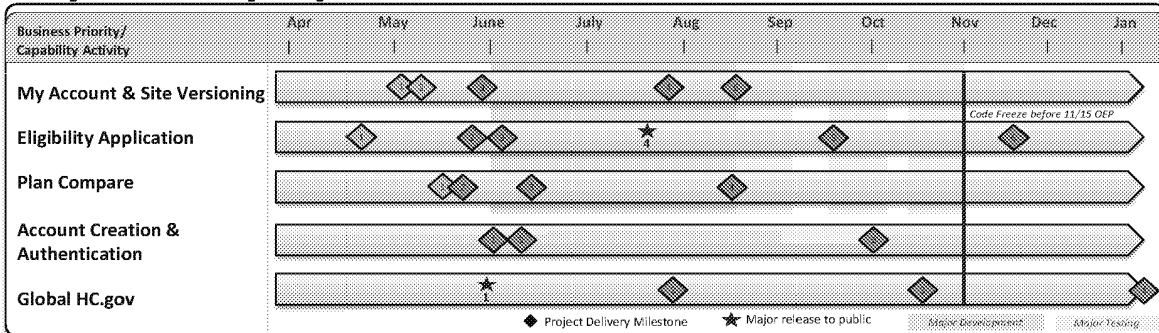
**End:** 5/21/2014 5:00:00 PM

**Show Time As:** Busy

**Recurrence:** (none)



# Key Priority Update: Consumer Tools - Highlights



#	My Account & 2015 Site Versioning	Plan	Actual
1	Draft consumer scenarios for user pathways through the site for 2014 & 2015 consumer activities	5/6	5/6
2	Draft conceptual wireframes for FFM Landing Page changes to support 2014 & 2015 consumer activities	5/9	5/9
3	Solidify Landing Page requirements, My Account requirements & basic 2015 versioning changes needed	5/30	
4	Complete development for 2015 versioning	7/25	
5	Testing Begins	8/15	

#	Eligibility Application	Plan	Actual
1	Ongoing CMS SME testing of Marketplace (MP) Application 2.0	Mid Apr – Mid June	
2	ATO issued for MP Application 2.0	5/23	
3	Finalize 2014 to 2015 logic for application copy/versioning to support consumers with an existing '14 application	6/6	
4	Go/No-Go & Initial public launch of Application 2.0 to 1% traffic	7/18	
5	Integrated In-depth ACA, UAT & Issuer Testing of Application 2.0 & FFM Classic Application with 2015 rules (round 2, round 3)	9/12 – 10/10 10/3 – 10/31	
6	Publish revised paper application	11/15	

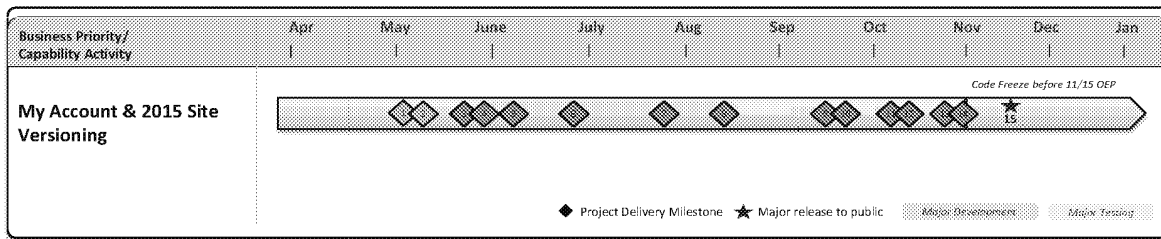
#	Plan Compare	Plan	Actual
1	Draft strategy for development integration for system flows across FFM & PC 2.0 elements	5/16	5/16
2	Finalize development contract mod for Plan Compare 2.0	5/20	
3	Complete business requirements for 2015 versioning	6/6	
4	FFM & MP 2.0 PC Development Complete – Conduct Integrated ACA, UAT, & Issuer testing using test data	8/15	

#	Account Creation & Authentication	Plan	Actual
1	Test migration strategy from EIDM to SLS	End of May	
2	Finalize strategy for Log In pathways for consumers vs. SHOP employer & employee accounts (FFM)	Late May – Early June	
3	Launch SLS – Production migration of consumer accounts	October 1	

#	Global HC.gov Changes	Plan	Actual
1	Non OEP Screener launch & Homepage changes – New Calls to Action (Screener, SHOP)	5/30	
2	Find Local Help – update data collection tool & enhance data & UX for improved consumer content	TBD Late Summer	
3	OEP Content & Information Architecture Changes	October	
4	Consumer Tax Tools	January	



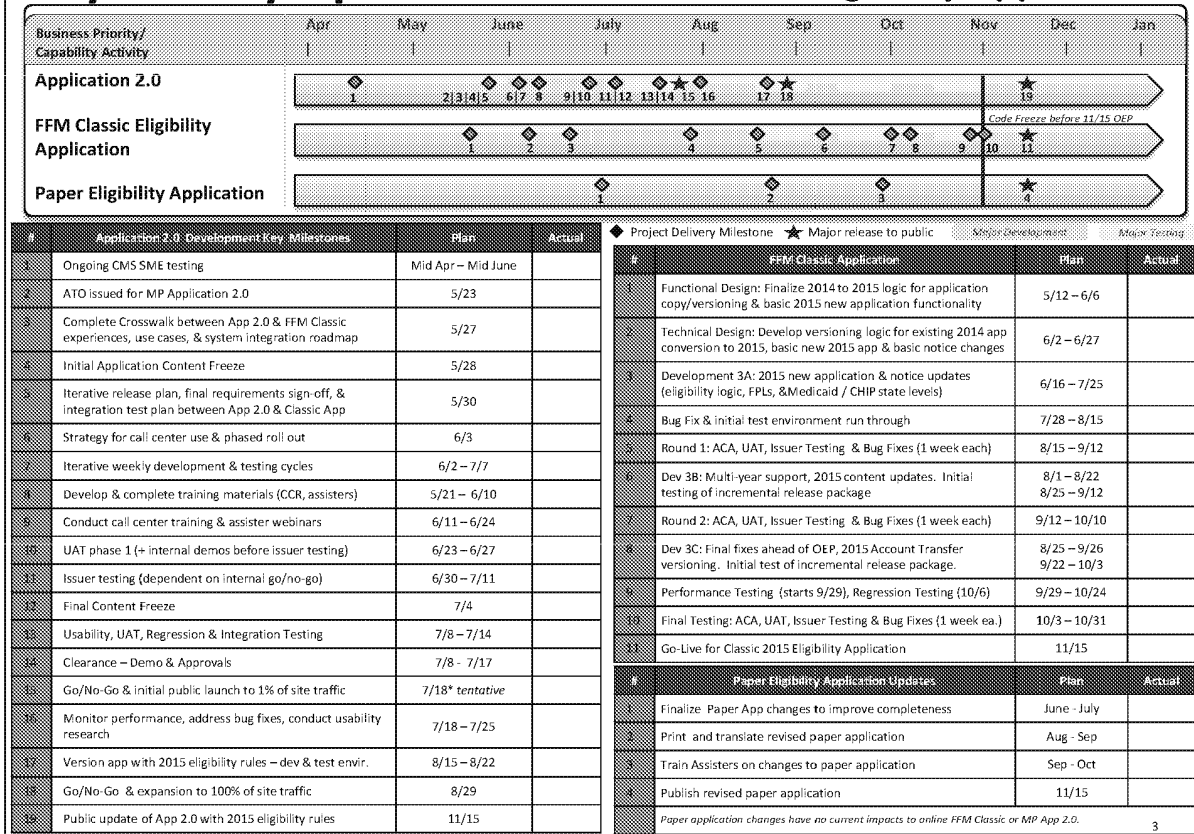
# Key Priority Update: Consumer Tools – My Account & 2015 Site Versioning



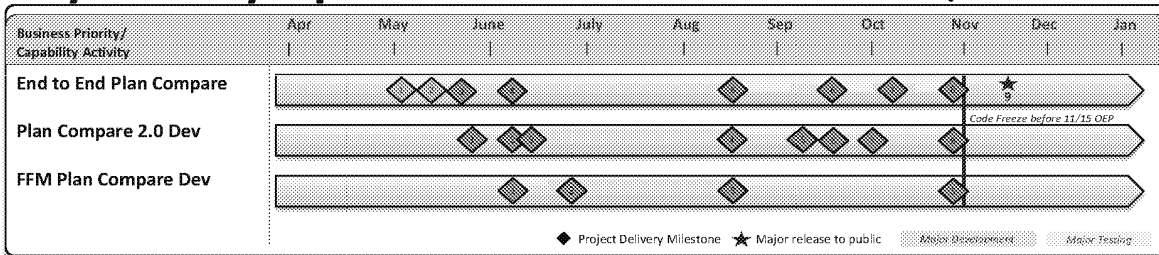
#	My Account & 2015 Site Versioning Key Milestones	Plan	Actual
1	Draft consumer scenarios for user pathways through the site for 2014 & 2015 consumer activities	5/6	5/6
2	Draft conceptual wireframes for FFM Landing Page changes to support 2014 & 2015 consumer activities	5/9	5/9
3	Inventory of changes & types of versioning needed by section within My Account	5/23	
4	Solidify Landing Page requirements, My Account requirements & basic 2015 versioning changes needed	5/30	
5	Functional Design Complete: My Account, Landing Page, web services for support channels 2015 versioning requirements finalized	6/6	
6	Technical Design Complete: 2015 basic consumer scenario through My Account & 2015 site versioning	6/27	
7	Development 3A: 2015 changes for Landing Page, My Account, overall FFM site versioning, updated call center web services	6/16 – 7/25	
8	Bug Fix & Initial test environment run through	7/28 – 8/15	
9	Round 1: ACA, UAT, Issuer Testing & Bug Fixes (1 week each)	8/15 – 9/12	
10	Dev 3B: Multi-year support, 2015 content updates. Initial testing of incremental release package	8/1 – 8/22   8/25 – 9/12	
11	Round 2: ACA, UAT, Issuer Testing & Bug Fixes (1 week each)	9/12 – 10/10	
12	Dev 3C: Final fixes ahead of OEP, 2015 Account Transfer & Direct Enrollment versioning. Initial test of incremental release package.	8/25 – 9/26   9/22 – 10/3	
13	Performance Testing (starts 9/29), Regression Testing (10/6)	9/29 – 10/24	
14	Final Testing: ACA, UAT, Issuer Testing & Bug Fixes (1 week ea.)	10/3 – 10/31	
15	Consumer Go-Live in production	11/15	



# Key Priority Update: Consumer Tools – Eligibility Application



# Key Priority Update: Consumer Tools – Plan Compare



#	End-to-End Plan Compare Milestones	Plan	Actual
1	Draft consumer flows for major consumer scenarios	5/6	5/6
2	Draft strategy for development integration for system flows across FFM & PC 2.0 elements	5/16	5/16
3	Kick off Plan Compare integration with PC 2.0 & FFM development teams	5/19 - 5/23	
4	Finalize development requirements between FFM & Plan Compare 2.0 system components (functional design complete)	6/6	
5	3A Testing: Integrated ACA, UAT, & Issuer testing using test/dummy data (1 week each, 4 <sup>th</sup> week is bug fix)	8/15 - 9/12	
6	3B Testing: In-depth ACA, UAT & Issuer testing with draft 2015 QHP data (1 week each, 4 <sup>th</sup> week is bug fix)	9/12 - 10/10	
7	3C Testing: Final ACA, UAT & Issuer Testing (1 week each, 4 <sup>th</sup> week is bug fix)	10/3 - 10/31	
8	Update production package with final, locked down QHP data	10/22 - 11/7	
9	Consumer Go-Live in production	11/15	

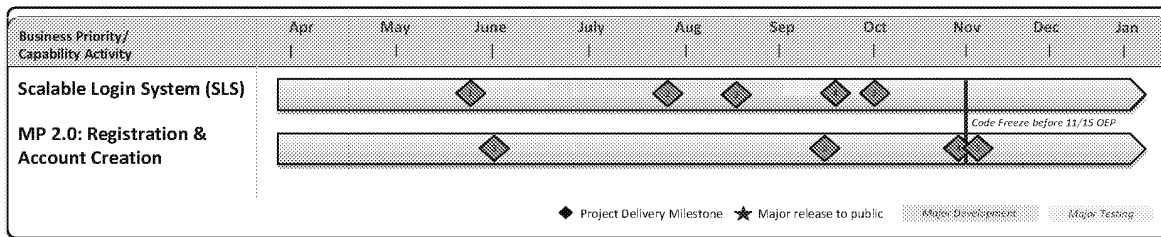
#	FFM Plan Compare Development Key Milestones	Plan	Actual
1	Draft 2015 changes needed to business logic for Enroll To-Do List, To-Do List Tasks, & backend services	6/6	
2	Complete technical requirements for 2015 versioning	6/27	
3	Initial development complete for 2015 plan compare	8/15	
4	Initial cut of draft 2015 QHP data	9/8	
5	Final cut of 2015 QHP data	10/21 - 11/4	

QHP data cuts dependent on PM milestones (ranges account for internal plan vs. public dates)

#	Plan Compare 2.0 Development Key Milestones	Plan	Actual
1	Finalize development contract mod	5/20	
2	Complete business requirements for PC 2.0 QHP data store	Early June	
3	Complete business requirements for PC 2.0 UI/UX	Early June	
4	Initial development complete	8/15	
5	Load initial draft 2015 QHP data	9/9 - 9/12	
6	Security Control Audit (SCA)	Mid-Sept	
7	ATO issued	10/1	
8	Load final 2015 QHP data	10/22 - 11/7	



# Key Priority Update: Consumer Tools – Account Creation & Authentication



#	SLS Milestones	Plan	Actual
1	Test migration strategy from EIDM	End of May	
2	Initial development complete	End of July	
3	Security Control Audit (SCA)	Mid-Aug	
4	ATO issued	Mid-Sept	
5	Launch (production migration)	October 1	

NOTE: dates are conservative and will be refined with dev team input over the next 2 weeks

#	Registration & Account Creation Milestones	Plan	Actual
	MP 2.0 – launched new account creation screens	Feb	Feb
1	MP 2.0 - 100% cutover for account creation screens from FFM to MP 2.0 Registration	TBD	
2	Finalize strategy for Log In pathways for consumers vs. SHOP employer & employee accounts	Late May – Early June	
3	FFM – Update Login page on HC.gov to include user role selection in test environments (consumer, employer, employee) – tentative pending strategy	Sept	
4	MP 2.0 - Update Account Creation to include SHOP Employer and SHOP Employee accounts ** (integrated with SHOP tower)	Oct - Nov	
5	FFM – release updated Log In strategy for multiple roles (consumer, employer, employee)	Oct - Nov	

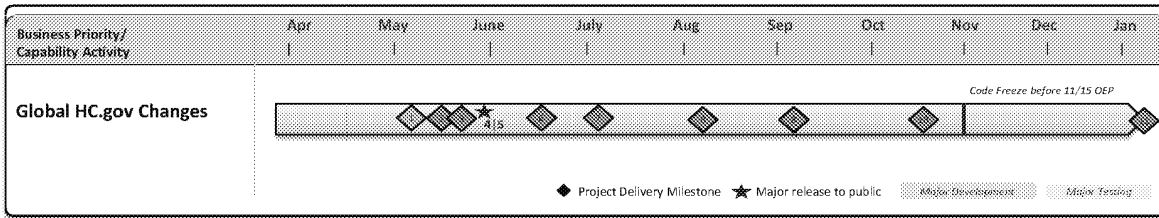
## STATUS UPDATE

- 5/16 Conducted cross-functional offsite on SLS Implementation Planning to dive into high level design discussions, identify business requirement needs, order of steps towards implementation, decisions or strategies that need to be finalized, & begin a deeper dive on technical architecture & system flows from current state (EIDM, FFM, RIDP) to future state (SLS, FFM, RIDP)
- Drafting systems inventory with key points of contact & high level timeline including major milestones & migration points
- Identifying required clearances, technical reviews, and any outstanding technical documentation requirements
- Identified data dependencies for final migration approach/options

## Upcoming Decision Points

- RIDP Integration Strategy (Business Decision) – SLS direct connection to RIDP or SLS integration with HUB to RIDP
- EIDM Account Migration Strategy – likely will require direct Oracle assistance in the next few weeks to assist in approach & actual migration
- Finalize SHOP integration between FFM, SLS, EIDM & how the user flow gets from the front end of HC.gov through account creation & log in to SHOP product for employers & employees. *Dependency: SHOP follow up conversation with IT resources, business owners & system owners*

# Key Priority Update: Consumer Tools – Global HC.gov



#	Global HC.gov Milestones	Plan	Actual
1	Draft consumer scenarios for user pathways through the site for 2014 & 2015 consumer activities	5/6	5/6
2	Non OEP Coverage Screener Tool Clearance Begins	Clearance Begins 5/14	[TBD: final clearance date]
3	Finalize visual refresh for Marketplace 2.0 look & feel	Late May – Early June	
4	Launch Non OEP Coverage Screener Tool	5/30	
5	Launch Healthcare.gov Homepage changes (new headline for screener, primary CTA changes to screener, secondary CTA changes to SHOP small business tools)	5/30	
6	Draft strategy for OEP information architecture to account for new consumer pathways & activities	Early – Mid June	
7	Launch HC.gov visual refresh for MP 2.0 (dependency: Application 2.0 launch)	Late June – Early July	
8	Find Local Help updates for data collection tool & improved consumer content	TBD Late Summer	
9	Develop content changes across site (consolidate, archive, reorganize, expand, new content for new consumer scenarios)	July - September	
10	Launch HC.gov OEP changes (new calls to action, updated information architecture, content revisions, etc)	October	
11	Consumer tax tools go-live	Late January	

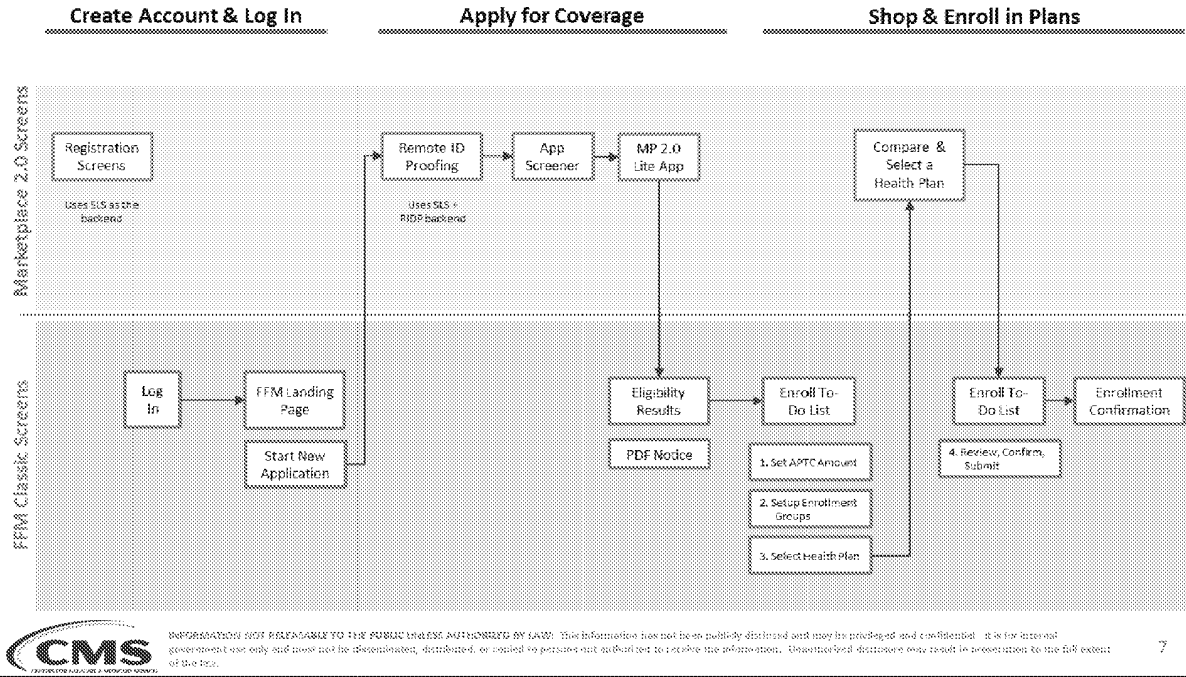




## Consumer Experience – Simple Case

Demonstrates the simplest case of a brand new user who is creating an account, applying and enrolling all in one sitting. There are additional steps in the process and parts of the site that the consumer would interact with to complete the application and enrollment process based on their situation

The flow below shows the interaction between Marketplace 2.0 and the FFM classic systems.



## Final Code Deployments

[illegible]

## High Level Cutover Tasks

#
1
2
3
2
3
4
5
6
7
8
9
10
11


Deployment
IMP1A deployment (Build#174 R7.0.0.9.7)
Prod Prime Hotfix
MIDAS deployment
MIDAS deployment
Prod Prime Deployment
Install ITM on PreProd Nodes and test process
MIDAS deployment
MIDAS deployment
??? FFM deployment: NotResp ???
??? FFM deployment to: NotResp
??? FFM deployment to PROD PRIME ???
??? FFM deployment: NotRes ???
??? FFM deployment to: NotRes ????
??? FFM deployment to PROD PRIME ???

Task
Integrate HC.gov learn and application side (protected page in front)
XML Gateway Audit, Cleanup Unused Firewalls, Create 3 IMPL environments
Cutover Prod Prime to Prod; Clear Test Data
NotResp Backup, VM Patching
Complete: NotResp Configuration
Complete FFM Configuration: NotRe L7, etc)
Database Upgrades, configure PROD support lifecycle, create PROD image in IM: NotResp
Finish cutover of PROD PRIME to PROD; Pull all existing Production data from FFM and DSH to get ready for Day1 deltas.
Application Layer Testing with Federal Partners/TDS
Coordinated Testing
Smoke Testing/Configuration Changes
Nexus Scan
Final cutover - publish web content
On-call support
On-call support
On-call support
On-call support
On-call support

On-call support
On-call support

Date	Status	Time
9/21/2013	Completed	
9/21/2013	Completed	
9/21/2013	Completed	
9/22/2013	Completed	
9/22/2013	Completed	
9/23/2013	Completed	
9/23/2013	Completed	
9/24/2013	Completed	
9/24/2013		
9/24/2013		
9/24/2013		
9/25/2013		
9/25/2013		
9/25/2013		

System/Stakeholder	Day	Timeframe
Healthcare.gov	Wednesday, September 25, 2013	
Hub	Wednesday, September 25, 2013	
MIDAS	Wednesday, September 25, 2013	
FFM	Wednesday, September 25, 2013	12:00am-6:00am
FFM	Wednesday, September 25, 2013	8:00am-8:00pm
FFM	Wednesday, September 25, 2013	8:00pm-12:00am
Hub	Thursday, September 26, 2013	
MIDAS	Thursday, September 26, 2013	
Federal Agencies	Thursday, September 26, 2013	
All	Thursday, September 26, 2013	8:00am-12:00pm
		12:00pm-8:00pm
		Friday
		Sunday
		Entire Period
		Entire Period
		Entire Period
		Entire Period
		Entire Period

		Entire Period
		Entire Period



Parties
OC
QSSI
MIDAS
URS
CGI
CGI
Hub
CGI, OC, Akamai, QSSI(F5, DSH, EIDM), CACI (MIDAS, Informatica)
CGI
URS

Akamai
OC
Adobe
CACI (Informatica, MIDAS)
EIDM

QSSI F5
QSSI DSH

	System	Area
1	HC.gov	Access
2	Hub	
3	Hub	
4	Hub	
5	MIDAS	
6	MIDAS	
	EIDM	
7	FFM	Access
8	FFM	URS
9	FFM	Prep
10	FFM	Prep
11	FFM	NotResp
12	FFM	
13	FFM	
14	FFM	
15	FFM	
16	FFM	
17	EIDM	
18	HC.gov	
19	HC.gov	
20	HC.gov	
21	EIDM	
22	EDIM	
23		
24	FFM	NotResp
25	FFM	
26	FFM	
27	FFM	
28	FFM	
29	FFM	

30	FFM	NotResp	
31	FFM		
32	FFM		
33	FFM		
34	FFM		
35	FFM		
36			
37			
38			
39			
40			
41			
42	FFM		
43	FFM		
44	FFM		
45	FFM		
46	FFM		
47	FFM		
48	FFM		
49	FFM	NotResp	(PZ and DZ)
50	FFM		(PZ and DZ)
51	FFM		(PZ and DZ)
52	FFM		(PZ and DZ)
53	FFM		(PZ and DZ)
54	FFM		(PZ and DZ)
55	FFM		(PZ and DZ)
56	FFM		(PZ and DZ)
57	FFM	Reverse Proxy	
58	Hub		
59	Hub		
60	Hub		
61	MIDAS		

62	MIDAS	
63	Federal Partners	
64	FFM	Reverse Proxy
65	FFM	Reverse Proxy
66	FFM	Reverse Proxy
67	FFM	Reverse Proxy
68	FFM	Reverse Proxy
69	FFM	Reverse Proxy
70	FFM	TC Cache (PZ)
71	FFM	L7 (PZ)
72	FFM	L7 (PZ)
73	FFM	L7 (PZ)
74	FFM	L7 (PZ)
75	FFM	L7 (PZ)
76	FFM	L7 (PZ)
77	FFM	L7 (AZ)
78	FFM	L7 (AZ)
79	FFM	L7
80	FFM	L7
81	HC.gov	
82	HC.gov	
83	FFM	L7 CCR
84	FFM	BRMS
85	FFM	NotResp
86	FFM	
87	FFM	
88	FFM	
89	FFM	
90	FFM	
91	FFM	
92	FFM	
93	FFM	FFM Infrastructure
94	FFM	FFM Infrastructure Ready
95	FFM	
96	FFM	FFM Infrastructure
97		Operational Readiness
98		Smoke Test
99		Operations
100		Operations
101	HC.gov	

102	HC.gov	
103	HC.gov	
104	HC.gov	
105	HC.gov	
106	HC.gov	
107	HC.gov	
108	HC.gov	
109	HC.gov	
110	HC.gov	
111	HC.gov	
112	HC.gov	
113	HC.gov	
114	HC.gov	
#REF!		Soft Launch
#REF!	HC.gov	

Task	
Integrate HC.gov learn and application side (protected page in front)	
Certificate/Partner Id audit on PreProd XML Gateways (On going, DSH Support team DSH Gateway teams are auditing certs/partnerids)	
Cleanup the unused firewall rules from SSG nodes, e.g. cleanup all the test FW rules from PreProd XML Gateway	
Create 3 IMPL environments with 8 VM pairs	
Start cutover of PROD PRIME to PROD(Dependency on FFM and DSH – Need confirmation from the upstream systems to	
Clear test data (Dependency on FFM and DSH – Need confirmation from the upstream systems to begin this work)	
Akamai test cutover	
Shutdown Reverse Proxies	
Patch several servers	
NotResp	Backup
	Backup
QHP/LOA PROD export	
Create ML Cluster	
Clear PRIME ML	
QHP/FM Export	
PROD Import	
FFM Setup	
Akamai imp cutover	
Integrate HC.gov learn and application side (protected page in front) (prodprime.healthcare.gov)	
Akamai staging changes for prodprime integration	
Push final 10/1 HealthCare.gov Learn code changes to test, imp, prodprime	
Akamai prod cutover	
SSL cert implementation	
Verification of Import	
Data Cleanup	
Verify IDL has correct ML end points (Data Pump)	
NotResp	Ready
NotResp	Backup
Configure PROD	NotResp as starting point



Verify/Create Folder Structure	
Copy PROD (QHP) to PROD	NotResp
Add QHP to PROD	NotResp
Update mount points	NotResp
Rebalance	NotResp
Verify Each mount Points	NotResp
Setup backup	
Ready	NotResp
Add additional VMs into Prod Cluster	NotResp
Verify configuration	NotResp
Verify using Admin	NotResp
Verify using JI (via service)	NotResp
Ready	NotResp
Verify schemas in PRIM	NotResp
Update End Points to new Cluster	NotResp
Update end points (LB in PZ)	NotResp
Verify correct Informatica endpoints	
Connection to TC ServerArray, TC Configuration	
Test and Verification	NotResp
Ready	NotResp
Correct Production Certificates	
Configure	NotResp
Database Upgrades	
Configure PROD support lifecycle	
Create PROD image in	NotResp
Finish cutover of PROD PRIME to PROD	

Pull all existing Production data from FFM and DSH to get ready for Day1 deltas. Need
Application Layer Testing with Federal Partners/TDS
Akamai verification/setup
Correct F5 (Load Balancing)
Pointing to PROD L7 Cluster
Webgate to EIDM PROD
Pointing to HIOS Prod
RP Ready
Configure PZ ServerArray
Layer7 Cluster
Configure to EIDM PROD
Connect to F5
Using TC Cache
English/Spanish
Layer 7 (PZ) Ready
Layer 7 (PZ) Cluster - add in add'l VMs (Elasticity)
Update to EIDM PROD (from IMPL)
Verification
Layer7 Completed
Hard freeze on content changes through 10/1
Final HealthCare.gov content push (10/1 release) to test, imp, prodprime environments
Complete configuration for CCR
BRMS in Load Balancer Mix
Verify FFM configuration
BRMS Ready
Verify configuration
NotResp Ready
Configure AZ ServerArray
Point QHP to new Cache
Modify EE <sup>notes</sup> to point to Cache
TC Cache in AZ Ready
FFM Infrastructure Ready
Coordinated-Partner Verification
NEXUS Scan
OR Activities
Verify PROD Infrastructure
Verify TWS Jobs
backups confirmed working
Merge HealthCare.gov branches - content, Find Local Help, and Help Center(English and Spanish) - to master

Deploy merged code to test, imp, prodprime environments

Validation testing/hotfix for blockers

Deploy merged code to prod-t (Terremark production)

HealthCare.gov Learn side ORR

Validation testing/hotfix for blockers in prod-t

End-to-end validation testing in prodprime environment

Akamai stage deployment (CGI code; not Learn side)

Spoof production testing (off CMS network; requires host file changes)

Continue spoof production testing (off CMS network; requires host file changes)

Akamai production deployment

Final HealthCare.gov content push (10/1 release) to prod environment

Akamai cache purge

Launch notifications

Soft Launch

Final cutover - publish web content

Status	Support	Dependency	Start
begin this work)			
			9:00 PM
	URS		
	URS		
	URS		
	URS	NotResp Backup	
Completed			
			9:00 PM
			9:00 AM
			11:00 AM
			6:00 PM
			9:00 PM
			9:00 PM
	IDL/CACI		

[illegible]

	Akamai, OC		
Completed	EIDM on call		
	HIOS on call		
	QSSI F5 on-call		
Completed			
Completed			
Completed			
Completed			
Completed	Akamai, OC		
Partial			
	Akamai, OC		
			0.708333333
			0.75
Completed			
		FFM Infrastructure Ready	
	URS		
			8:00 AM



			4:00 PM
			5:00 PM
			9:00 PM
			10:00 PM
			10:00 PM
			8:00 AM
			9:00 AM
			12:00 PM
			8:00 AM
			7:00 PM
			11:30 PM
			11:45 PM
			12:00 AM

Stop	Best Case Time Time	Worse Case Time	Completion Period
12:00 AM			
			1
			1
			1
			1
			1
			0
			2
			2
			2
			2
12:00 AM			
10:00 AM			
2:00 PM			
7:00 PM			
12:00 AM			
12:00 AM			
			3
			3
			3
	4	10	3
			1
			2

			2
	4	8	3
			3
			3
	4	8	4
			5
			6
	6	12	5
			5
			5
			5
			5
	4	6	5
			0
			4
			4
			4
			4
			5
	4	8	5
			4
			X

			8
			7
			7
			0
			7
			8
			4
			0
			6
			6
			6
			7
			7
			0
			7
			8
	6	8	8
ongoing			
0.791666667			
			?
			0
			4
			4
			5
			5
			5
			5
			5
			5
			7
			9
			14
			8
			9
			8
12:00 PM			

5:00 PM			
9:00 PM			
10:00 PM			
11:00 PM			
12:00 AM			
9:00 PM			
12:00 PM			
9:30 PM			
5:00 PM			
10:00 PM			
12:00 AM			
12:00 PM			
			16

Timeframe	Lead
Wednesday	OC
	QSSI
	QSSI
	QSSI
	CACI
	CACI
Monday	
Tuesday- Wednesday-Overnight	CGI
Tuesday- Wednesday-Overnight	URS
Tuesday- Wednesday-Overnight	URS
Tuesday- Wednesday-Overnight	URS
Tuesday- Wednesday-Overnight	Damon/Brian
Prep	Damon/Brian
Wednesday 8:00am-12:00pm	Damon/Brian
Wednesday 8:00am-12:00pm	Damon/Brian
Wednesday 8:00am-12:00pm	Damon/Brian
Wednesday 8:00am-12:00pm	Damon/Brian
Tuesday	
Wednesday	CGI
Wednesday	OC
Wednesday	OC
Wednesday	EIDM
Wednesday	EIDM
Wednesday 12:00pm-4:00pm	Damon/Brian
Wednesday 12:00pm-4:00pm	Damon/Brian
Wednesday 12:00pm-4:00pm	Damon/Brian
Wednesday 12:00pm-4:00pm	Damon/Brian
Tuesday- Wednesday-Overnight	
Wednesday 8:00am-12:00pm	Pat



Wednesday 8:00am-12:00pm	Pat
Wednesday 12:00pm-4:00pm	Pat
Wednesday 12:00pm-4:00pm	Pat
Wednesday 12:00pm-4:00pm	Pat
Wednesday 4:00pm-8:00pm	Pat
Wednesday 8:00pm-12:00am	Pat
Thursday 12:00am-4:00am	Pat
Wednesday 8:00pm-12:00am	Pat
Wednesday 8:00pm-12:00am	Pat
Wednesday 8:00pm-12:00am	Pat
Wednesday 8:00pm-12:00am	Pat
Wednesday 8:00pm-12:00am	Pat
Wednesday 8:00pm-12:00am	Pat
Prep	Joel
Wednesday 4:00pm-8:00pm	Joel
Wednesday 4:00pm-8:00pm	Joel
Wednesday 4:00pm-8:00pm	Joel
Wednesday 4:00pm-8:00pm	Joel
Wednesday 8:00pm-12:00am	Joel
Wednesday 8:00pm-12:00am	Joel
Wednesday 4:00pm-8:00pm	Joel
Delayed	XXXX
	QSSI
	QSSI
	QSSI
	CACI

	CACI
Thursday 8:00am-12:00pm	Jeremy
Thursday 4:00am-8:00am	Jeremy
Thursday 4:00am-8:00am	Jeremy
Prep	Jeremy
Thursday 4:00am-8:00am	Jeremy
Thursday 8:00am-12:00pm	Jeremy
Wednesday 4:00pm-8:00pm	Trevor
Prep	Balaji
Thursday 12:00am-4:00am	Balaji
Thursday 12:00am-4:00am	Balaji
Thursday 12:00am-4:00am	Balaji
Thursday 4:00am-8:00am	Balaji
Thursday 4:00am-8:00am	Balaji
Prep	Balaji
Thursday 4:00am-8:00am	Balaji
Thursday 8:00am-12:00pm	Balaji
Thursday 8:00am-12:00pm	Balaji
Delayed	Balaji
Prep	Joel
Wednesday 4:00pm-8:00pm	Joel
Wednesday 4:00pm-8:00pm	Joel
Wednesday 8:00pm-12:00am	Pat
Wednesday 8:00pm-12:00am	Pat
Wednesday 8:00pm-12:00am	Trevor
Wednesday 8:00pm-12:00am	Trevor
Wednesday 8:00pm-12:00am	Trevor
Wednesday 8:00pm-12:00am	Trevor
Thursday 4:00am-8:00am	Joel, Keith
Thursday 12:00pm-4:00pm	Joel, Keith
Friday 8:00am-12:00pm	Balaji
Thursday 8:00am-12:00pm	Taulant
Thursday 12:00pm-4:00pm	Mazen
Thursday 8:00am-12:00pm	Taulant
Friday	

Friday	
Friday	
Friday	
Friday	
Friday	
Saturday	
Sunday	
Sunday	
Monday	
Monday	
Monday	
Monday	
Monday	
Monday	
Friday 4:00pm-8:00pm	
	OC

Notes
- prevent access once backups start
- Setup FFM - normal deployment process
- security script
- Hub OPM/PC data
- run queries, compare from original QHP and FFM
- Hub test against OPM/PC
As data comes from PM/FM, is there anything to clean up?
For Content Pump
- IDL Test
- Clean up existing data
- New Folder Structure
- Logical Volumes

- FFM Folders
- EFT Folders (need storage/folder requirements from EFT)
- DSH Folders
NotResp
- Copy to centralized FS for pickup
- can occur after NotResp is up
- includes App Zone and Data Zone NotResp
Maintain separate NotResp continue using Prime NotResp
- Trevor has this, may wait
- memory leak patch
NotResp Logging not at Debug - confirm Info
- ulimit on NotResp /Ms set correctly
- convert HIX to Prod (as used in LOA)
- configure NotResp (Collector, Transmitter on RPs)
- need FW to servers at XOC

- ready by 8:00am, Thursday
- ready by 8:00am, Thursday
- ready by 8:00am, Thursday
12 hours
Trevor has this
- EE using separate BRMS from QHP, already setup in PRIME
- Verify tuning configuration from Peter L
Trevor has this
- ready by 8:00am for coordination testing with Akamai and others
-8:00am-4:00pm
- functional readiness tasks
- Test Integrations (Akamai, Agent/Brokers, CCR, Hub, etc)
- test LOA accounts continue to work
Notes
Backups
NotResp Backups
NotResp Backups

**Blank Page**



Risk
- confirm what VMs they are patching
- configuring all end points back to new instance

[illegible]

**Blank Page**

**Blank Page**

<i>Start Time</i>	<i>End Time</i>	<i>Revised Start Time</i>	<i>Revised End Time</i>
<b>Fri, Sep 20, 2013</b>			
<b>NotResp Deployment</b>			
4:00 PM	6:00 PM		
6:00 PM	7:00 PM		
7:00 PM	9:45 PM		
9:45 PM	10:15 PM		
10:15 PM	12:15 PM		
<b>Sat, Sep 21, 2013</b>			
<b>Hotfix to PROD PRIME</b>			
6:00 PM	1:00 AM		
1:00 AM	2:00 AM		
2:00 AM	4:00 AM		
4:00 AM	5:00 AM		
5:00 AM	6:00 AM		
8:00 AM	10:00 AM		
<b>Hub</b>			
5:00 PM	5:00 PM		
9:30 PM	10:30 PM		
10:30 PM	11:00 PM		
9:30 PM	9:30 PM		
<b>MIDAS</b>			
2:00 PM	7:00 PM		
7:00 PM	12:00 AM		
5:00 PM	12:00 AM		
11:00 PM	11:30 PM		
11:30 PM	12:00 AM		
<b>Sun, Sep 22, 2013</b>			
<b>Hub</b>			
11:00 PM	2:00 AM		
11:00 PM	2:00 AM		
2:00 AM	2:00 AM		
2:00 AM	3:00 AM		
3:00 AM	3:15 AM		
3:15 AM	4:00 AM		
4:00 AM	4:00 AM		
<b>MIDAS</b>			
11:00 AM	12:00 PM		
12:00 AM	1:00 PM		
12:00 PM	1:00 PM		
2:00 PM	3:00 PM		
<b>Mon, Sep 23, 2013</b>			
<b>Hub</b>			
<b>MIDAS</b>			
12:00 PM	1:00 PM		
12:00 PM	1:00 PM		
12:00 PM	1:00 PM		
2:00 PM	3:00 PM		
<b>FFM</b>			

Tue, Sep 24, 2013			
MIDAS			
	9:00 AM	10:00 AM	
	9:00 AM	10:00 AM	
	10:00 AM	11:00 AM	
	11:00 AM	1:00 PM	
FFM			

#REF!				
HC.gov	7:00 AM	7:00 AM		

Activity
<p>Deploy</p> <p>Deploy Hotfixes</p> <p>Update <b>NotRes</b> Plan Data</p> <p>Conduct End-to-End Test with Issuer Data</p> <p>Finish smoke testing and resolve any issues</p>
<p>Bring down Prod Prime</p> <p>Deploy to Prod Prime with Hotfixes</p> <p>Conduct End-to-End Test with Issuer Data</p> <p>Preparation for Sunday Performance Test</p> <p>Finish smoke testing and resolve any issues</p> <p>Environment available for ACA team</p>
<p>Create HUB CR for Code and <b>NotResp</b> Deployment to PROD'</p> <p>Backup <b>NotR</b> database servers</p> <p>Backup build artifacts from the <b>NotRes</b> deployments directory</p> <p>Check-in correct <b>NotRes</b> property files in xoc-jenkins in SVN</p>
<p>Create updated DDL database release</p> <p>Create updated TSV2 HIVE queries release</p> <p>Create new <b>NotRes</b> BI reports release for defect fixes</p> <p>Deploy latest OEM release to Prod Prime for testing</p> <p>Deploy latest ETL TSV1 release to Prod Prime for internal testing</p>
<p>Deploy new build artifacts to the <b>NotR</b> deployments directory (Appzone and Datazone)</p> <p>Deploy new build to <b>NotR</b> database server (DB01)</p> <p>Bring up <b>NotResp</b> les and notify CMS, Hub and CGI.</p> <p>Run Smoke tests against Test Harness</p> <p>Switch Endpoints for Fetch Eligibility and Direct Enrollment to real endpoints.</p> <p>Run Smoke tests against real endpoints.</p> <p>Notify CMS, Hub and CGI of test results</p> <p>Test the network connectivity from PreProd XML Gateway nodes to TDS Production endpoints.</p>
<p>Deploy updated DDL database release to Prod Prime</p> <p>Deploy updated TSV2 HIVE queries release to Prod Prime</p> <p>Deploy new <b>NotRes</b> BI reports release to <b>NotRes</b> and perform internal testing</p> <p>Deploy new <b>NotResp</b> BI reports release to Prod Prime and perform internal testing</p>
<p>Install ITM on PreProd Nodes and test process</p>
<p>Deploy any updated DDL database release to <b>NotR</b> and Prod Prime</p> <p>Deploy any updated TSV2 release to <b>Not</b> Prod Prime</p> <p>Deploy any new <b>NotResp</b> BI reports release to <b>NotR</b> and Prod Prime</p> <p>Deploy new OEM Report release to <b>NotR</b> and Prod Prime</p>
<p>Deploy FFM build to <b>NotResp</b></p>



Smoke test in [NotRes]  
Deploy FFM build to [p] [NotRes]  
Smoke test in [NotRes]  
Deploy FFM build to PROD PRIME  
Smoke test in PROD PRIME

Deploy updated DDL database release to support additional MMI metrics to [NotRe] and Prod Prime  
Deploy updated TSV2 release to support additional MMI metrics to [NotRe] and Prod Prime  
Deploy updated OEM Report and [NotResp] reports release to support additional metrics to [NotRe] and Prod Prime  
Deploy new DSH Reports release to [NotRes] and Prod Prime

Deploy FFM build to [NotResp]  
Smoke test in [NotRes]  
Deploy FFM build to [NotResp]  
Smoke test in [NotResp]  
Deploy FFM build to PROD PRIME  
Smoke test in PROD PRIME

Final cutover - publish web content

<i>Status</i>	<i>System</i>	<i>Team Responsible</i>	<i>Notes/Release Number</i>
Complete	FFM	CGI	Build#174 R7.0.0.9.7
Complete	FFM	CGI	Build#174 R7.0.0.9.7
Complete	FFM	CGI	Build#174 R7.0.0.9.7
Complete	FFM	CGI	Build#174 R7.0.0.9.7
Complete	FFM	CGI	Build#174 R7.0.0.9.7
Complete	FFM	CGI	
Complete	FFM	CGI	
Complete	FFM	CGI	
Complete	FFM	CGI	
Complete	FFM	CGI	
Complete	Hub	QSSI	
Complete	Hub	QSSI	
Complete	Hub	QSSI	
Complete	Hub	QSSI	
Complete	FFM	QSSI	
Complete	FFM	QSSI	
Complete	FFM	QSSI	
Complete	FFM	QSSI	
Complete	FFM	QSSI	
Complete	FFM	QSSI	
Complete	FFM	QSSI	
Complete	MIDAS	CACI	
Complete	MIDAS	CACI	
Complete	MIDAS	CACI	
Complete	MIDAS	CACI	
	Hub	QSSI	
	MIDAS	CACI	
	MIDAS	CACI	
	MIDAS	CACI	
	MIDAS	CACI	
	FFM	CGI	

	FFM	CGI
	FFM	CGI
	FFM	CGI
	FFM	CGI
	FFM	CGI
	MIDAS	CACI
	MIDAS	CACI
	MIDAS	CACI
	MIDAS	CACI
	FFM	CGI
	FFM	CGI
	FFM	CGI
	FFM	CGI
	FFM	CGI
	FFM	CGI

	HC.gov	OC	

Period	Description			
0	Prep			
1	Tuesday- Wednesday-Overnight	Tuesday-	Wednesday	Overnight
2	Wednesday 8:00am-12:00pm	Wednesday	8:00am	12:00pm
3	Wednesday 12:00pm-4:00pm	Wednesday	12:00pm	4:00pm
4	Wednesday 4:00pm-8:00pm	Wednesday	4:00pm	8:00pm
5	Wednesday 8:00pm-12:00am	Wednesday	8:00pm	12:00am
6	Thursday 12:00am-4:00am	Thursday	12:00am	4:00am
7	Thursday 4:00am-8:00am	Thursday	4:00am	8:00am
8	Thursday 8:00am-12:00pm	Thursday	8:00am	12:00pm
9	Thursday 12:00pm-4:00pm	Thursday	12:00pm	4:00pm
10	Thursday 4:00pm-8:00pm	Thursday	4:00pm	8:00pm
11	Thursday 8:00pm-12:00am	Thursday	8:00pm	12:00am
12	Friday 12:00am-4:00am	Friday	12:00am	4:00am
13	Friday 4:00am-8:00am	Friday	4:00am	8:00am
14	Friday 8:00am-12:00pm	Friday	8:00am	12:00pm
15	Friday 12:00pm-4:00pm	Friday	12:00pm	4:00pm
16	Friday 4:00pm-8:00pm	Friday	4:00pm	8:00pm
17	Friday 4:00pm-12:00am	Friday	4:00pm	12:00am
X	Delayed			
?	TBD			

#	Task
1	Restore MarkLogic from backup
2	Restore Oracle from backup
3	Restore Alfresco from backup
4	Restrict access to PROD-EE (via Akamai). Allow only internal/CMS testing to continue
5	Only allow access via Portal/HIOS to PM/FM
6	
7	

#	Strategy
1	FM/PM will remain on the same VMs as currently in PROD (minimizes impact on PM/FM)
2	
3	

Appointment

**From:** Amos, Robert E. (CMS/OC) [NotResp]  
 [NotResp]  
**Sent:** 9/9/2013 1:00:20 PM  
**To:** Amos, Robert E. (CMS/OC) [NotResp]  
 [NotResp] Banerjee, Dharitri (CGI Federal)  
 (dharitri.banerjee@cgifederal.com) [dharitri.banerjee@cgifederal.com]; Weiss, Paul (CGI Federal)  
 [Paul.Weiss@cgifederal.com]; Trefzger, William (CMS/DWO) [NotResp]  
 [NotResp]; Burch, Mimi Z. (CMS/OC) [NotResp]  
 [NotResp] Asplen, Suzanne W. (CMS/CPI) [NotResp]  
 [NotResp] Starry, Melissa A. (CMS/OIS) [NotResp]  
 [NotResp] Ramsey, Letticia T.(CMS/OC) [NotResp]  
 [NotResp] Mitchell, Michael F. (CMS/OC)  
 [NotResp] Tudor, Susan J. (CMS/OC)  
 [NotResp] Booth, Jon G. (CMS/OC)  
 [NotResp] Patel, Ketan (CMS/OC)

**Subject:** Walk through PROD PRIME Functionality List  
**Location:** Call & Web [ (b)(6) ] (Meeting Number [ (b)(6) ])

**Start:** 9/9/2013 2:00:00 PM

**End:** 9/9/2013 2:30:00 PM

**Show Time As:** Tentative

**Recurrence:** (none)

**Required Attendees:** Banerjee, Dharitri (CGI Federal) (dharitri.banerjee@cgifederal.com); Weiss, Paul (CGI Federal); Trefzger, William (CMS/DWO); Burch, Mimi Z. (CMS/OC); Asplen, Suzanne W. (CMS/CPI); Starry, Melissa A. (CMS/OIS); Ramsey, Letticia T.(CMS/OC); Mitchell, Michael F. (CMS/OC); Tudor, Susan J. (CMS/OC); Booth, Jon G. (CMS/OC); Patel, Ketan (CMS/OC)

Web if needed: [https://\[ \(b\)\(6\) \]](https://[ (b)(6) ])

EE\_Build\_functionlity map\_9\_6.xlsm FFM BuildNotes FFE Rel 7.0.0.6, 7.0.0.7, 7.0.0.7.1 -161-Sep 06 2013 - Pr....doc

**From:** Amos, Robert E. (CMS/OC)  
**Sent:** Monday, September 09, 2013 8:43 AM  
**To:** Banerjee, Dharitri (CGI Federal); Trefzger, William (CMS/DWO)  
**Cc:** Booth, Jon G. (CMS/OC); Patel, Ketan (CMS/OC); Burch, Mimi Z. (CMS/OC); Tudor, Susan J. (CMS/OC); Weiss, Paul (CGI Federal)  
**Subject:** RE: Fwd: CGI Deployment Notification - E&E PROD PRIME Sunday September 08, 2013

Dharitri,

Did a quick scan of the file you sent – on the 9:45am call we'll want to make sure it's clear how to view all functionality in the current deployment of PROD PRIME that we'll be UATING this week.

Thx  
 Bob



**From:** Banerjee, Dharitri (CGI Federal) [<mailto:dharitri.banerjee@cgifederal.com>]

**Sent:** Monday, September 09, 2013 8:14 AM

**To:** Trefzger, William (CMS/DWO); Amos, Robert E. (CMS/OC)

**Cc:** Booth, Jon G. (CMS/OC); Patel, Ketan (CMS/OC); Burch, Mimi Z. (CMS/OC); Tudor, Susan J. (CMS/OC); Weiss, Paul (CGI Federal)

**Subject:** RE: Fwd: CGI Deployment Notification - E&E PROD PRIME Sunday September 08, 2013

Yes, I am targeting to get our CGI team to be on the call.

Bob- lets meet at 9:45 then?



Dharitri Banerjee, MS, PMP, CSM| W: 703-227-7270| C: (b)(6) [www.cgi.com](http://www.cgi.com)

**From:** trefzger, william

**Sent:** Monday, September 09, 2013 8:09 AM

**To:** Banerjee, Dharitri (CGI Federal); Amos, Robert E. (CMS/OC)

**Cc:** booth, jon; Patel, Ketan; Burch, Mimi Z. (CMS/OC); Tudor, Susan J. (CMS/OC); Weiss, Paul (CGI Federal)

**Subject:** RE: Fwd: CGI Deployment Notification - E&E PROD PRIME Sunday September 08, 2013

Yes, QSSI is given the assignment for the walkthrough.

However, it is based on their experience in **NotResp** at Prod Prime, so it is not uncommon for some specifics to ProdPrime are overlooked and our UAT does not get off to a smooth start as a result. Also, as noted in other emails from Bob and Mimi, we have not been getting complete documentation on what is in the release. Gentle reminder: understanding the status of the release vis a vis IE8 is critical.

So if CGI folks could be on the call to fill in the blanks, that would be great.

As soon as Galina sends it out, we'll make sure you have it. 10:00 is the target.

thanks

**From:** Banerjee, Dharitri (CGI Federal) [<mailto:dharitri.banerjee@cgifederal.com>]

**Sent:** Monday, September 09, 2013 6:15 AM

**To:** Amos, Robert E. (CMS/OC); Trefzger, William (CMS/DWO)

**Cc:** Booth, Jon G. (CMS/OC); Patel, Ketan (CMS/OC); Burch, Mimi Z. (CMS/OC); Tudor, Susan J. (CMS/OC); Weiss, Paul (CGI Federal)

**Subject:** RE: Fwd: CGI Deployment Notification - E&E PROD PRIME Sunday September 08, 2013

Thank you Bob. I am guessing QSSI is doing the walkthrough?



Dharitri Banerjee, MS, PMP, CSM| W: 703-227-7270| C: (b)(6) [www.cgi.com](http://www.cgi.com)

**From:** Amos, Robert E. (CMS/OC) [<mailto:Robert.Amos@cms.hhs.gov>]

**Sent:** Monday, September 09, 2013 5:54 AM

**To:** Banerjee, Dharitri (CGI Federal); trefzger, william

**Cc:** booth, jon; Patel, Ketan; Burch, Mimi Z. (CMS/OC); Tudor, Susan J. (CMS/OC)

**Subject:** Re: Fwd: CGI Deployment Notification - E&E PROD PRIME Sunday September 08, 2013

Dharitri,

Thanks. No invite yet from Galina; we'll forward as soon as we get it.

Thx

Bob

**From:** Banerjee, Dharitri (CGI Federal) [<mailto:dharitri.banerjee@cgifederal.com>]

**Sent:** Sunday, September 08, 2013 08:34 PM

**To:** Amos, Robert E. (CMS/OC); Trefzger, William (CMS/DWO)

**Cc:** Booth, Jon G. (CMS/OC); Patel, Ketan (CMS/OC); Burch, Mimi Z. (CMS/OC); Tudor, Susan J. (CMS/OC)

**Subject:** RE: Fwd: CGI Deployment Notification - E&E PROD PRIME Sunday September 08, 2013

Bob- sorry for the delay in responding. I have just received the confirmed list of functionality that has gone into the deployment (see attached). Also, please note that the testers are in the process of completing all tests, following which, I will be able to send out the list of known issues with workarounds, if any.

Bill- following up on our conversation, please forward me Galina's invite for the walkthrough tomorrow.

Thanks,

Dharitri



Dharitri Banerjee, MS, PMP, CSM| W: 703-227-7270| C: (b)(6) | [www.cgi.com](http://www.cgi.com)

**From:** Amos, Robert E. (CMS/OC) [<mailto:Robert.Amos@cms.hhs.gov>]

**Sent:** Sunday, September 08, 2013 3:22 PM

**To:** Banerjee, Dharitri (CGI Federal); trefzger, william

**Cc:** booth, jon; Patel, Ketan; Burch, Mimi Z. (CMS/OC); Tudor, Susan J. (CMS/OC)

**Subject:** Re: Fwd: CGI Deployment Notification - E&E PROD PRIME Sunday September 08, 2013

Thanks for this heads up. Dharitri, do we have the list of complete functionality going into PROD PRIME today?

Thx

Bob

**From:** Banerjee, Dharitri (CGI Federal) [<mailto:dharitri.banerjee@cgifederal.com>]

**Sent:** Sunday, September 08, 2013 12:46 PM

**To:** Amos, Robert E. (CMS/OC); Trefzger, William (CMS/DWO)

**Subject:** Fwd: CGI Deployment Notification - E&E PROD PRIME Sunday September 08, 2013

FYI

Sent from my iPhone

Begin forwarded message:

**From:** "Bartolotti, Larry (CGI Federal)" <Larry.Bartolotti@cgifederal.com>**Date:** September 8, 2013, 12:08:23 PM EDT

**To:** "Oh, Mark U. (CMS/OIS)" <mark.oh@cms.hhs.gov>, "Margush, Doug C. (CMS/OIS)" <douglas.margush@cms.hhs.gov>, "Dill, Walter (CMS/OIS)" <Walter.Dill2@CMS.hhs.gov>, "Donohoe, Paul X. (CMS/OIS)" <Paul.Donohoe@cms.hhs.gov>, "Carter, Cheryl K (CGI Federal)" <Cheryl.Carter@cgifederal.com>, "dbhatta@qssinc.com" <dbhatta@qssinc.com>, "mnaik@qssinc.com" <mnaik@qssinc.com>, "Walker, Benjamin L. (CMS/CCIIO)" <benjamin.walker@cms.hhs.gov>, "Zaman, Akhtar (CMS/OIS)" <Akhtar.Zaman@cms.hhs.gov>

**Cc:** "James, Brian M. (CMS/CCIIO)" <brian.james@cms.hhs.gov>, "Thompson, Tyrone (CMS/OIS)" <tyrone.thompson2@cms.hhs.gov>, "Walter, Stephen J. (CMS/OIS)" <stephen.walter@cms.hhs.gov>, "Shropshire, Richard (CMS/CCIIO)" <richard.shropshire@cms.hhs.gov>, "Cummings, Duane (CGI Federal)" <Duane.Cummings@cgifederal.com>, "Thurston, Robert (CMS/CTR)" <Robert.Thurston@cms.hhs.gov>, "peter@t1cg.com" <peter@t1cg.com>, "Van, Hung B. (CMS/OIS)" <Hung.Van@cms.hhs.gov>, "De Moura, Jesse (CGI Federal)" <Jesse.De.Moura@cgifederal.com>, FFM-Build Deployment <FFMBuildDeployment@cgifederal.com>, "Calem, Mark (CGI Federal)" <Mark.Calem@cgifederal.com>, "Neidecker, Bob (CGI Federal)" <Bob.Neidecker@cgifederal.com>, "Sharma, Hemant (CGI Federal)" <Hemant.Sharma@cgifederal.com>, "Halkedis, John (CGI Federal)" <John.Halkedis@cgifederal.com>, "Kodavaluru, Radha (CGI Federal)" <radha.kodavaluru@cgifederal.com>, "Kutsilev, Lubo (CGI Federal)" <lubo.kutsilev@cgifederal.com>, "Sousa, Steven (CGI Federal)" <Steven.Sousa@cgifederal.com>, "Banerjee, Dharitri (CGI Federal)" <dharitri.banerjee@cgifederal.com>, "Jones, Lynn B." (lbjones@mitre.org)" <lbjones@mitre.org>, "Dinakaran, Sai (CGI Federal)" <sai.dinakaran@cgifederal.com>, "Couts, Todd (CMS/OIS)" <Todd.Couts1@cms.hhs.gov>, "Cole, Reba R. (CMS/OIS)" <Reba.Cole@cms.hhs.gov>

**Subject:** CGI Deployment Notification - E&E PROD PRIME Sunday September 08, 2013

The Deployment to Prod Prime is starting now.

Sunday 9/8/2013

Time	Activity	ENV	Status
Now – 12:00pm	Verification of current code in Prod Prime	Prod Prime	Complete
12:00pm – 2:00pm	Deployment of Release 7.0.0.7.1	Prod Prime	In Progress
2:00pm – 5:00pm	Smoke Test and validate demo scenario	Prod Prime	Pending
5:00pm	Pre walk-thru of demo with CMS	Prod Prime	Pending
7:00pm	Demo with Henry	Prod Prime	Pending

Thanks,  
Larry

\_\_\_\_\_  
Lawrence V. Bartolotti | CGI - Federal, Inc | office 703.227.6969 | mobile  
larry.bartolotti@cgifederal.com

(b)(6)

CMS000804

Robert Amos invites you to an online meeting using WebEx.

Meeting Number: (b)(6)

Meeting Password: This meeting does not require a password.

---

Audio conference information

---

1. Please call the following number:

WebEx: (b)(6)

2. Follow the instructions you hear on the phone.

Your WebEx Meeting Number: (b)(6)

---

To join from the Baltimore, Chicago, or Kansas City offices

---

1. Dial ext. (b)(6)

2. Enter the Meeting Number: (b)(6)

---

To join this meeting online

---

1. Go to [https://\(b\)\(6\)](https://(b)(6))

2. If requested, enter your name and email address.

3. If a password is required, enter the meeting password: This meeting does not require a password.

4. Click "Join".

5. Follow the instructions that appear on your screen.



Centers for Medicare & Medicaid Services  
Center for Consumer Information and Insurance Oversight  
7500 Security Blvd  
Baltimore, MD 21244-1850

## Federally Facilitated Marketplace (FFM) Build Notes (Release 7.0.0.6, 7.0.0.7, 7.0.0.7.1)

**Version:** 1.0  
**Last Modified:** 9/07/2013

**Contract Number:** HHSM-500-T0012

{ STYLEREf Module/Acronym \\* MERGEFORMAT }

## APPROVALS

### Submitting Organization's Approving Authority:

---

Signature	Printed Name	Date	Phone Number
<hr/>			

### CMS' Approving Authority:

---

Signature	Printed Name	Date	Phone Number
<hr/>			



## TABLE OF CONTENTS

<b><u>1.</u></b>	<b><u>Introduction</u></b>	<b>1</b>
1.1.	Purpose	1
1.2.	Audience	1
1.3.	Build Manifest	1
<b><u>2.</u></b>	<b><u>New Features and Fixed Issues</u></b>	<b>1</b>
2.1.	New Features	1
2.1.1.	Individual Application	1
2.1.2.	My Account	4
2.1.3.	Plan Compare	6
2.1.4.	ESD	6
2.1.5.	Direct Enrollment API	7
2.1.6.	Call Center Development	7
2.1.7.	Enrollment	7
2.1.8.	Financial Management	8
2.2.	Resolved Defects	9
2.3.	System Access	9
<b><u>3.</u></b>	<b><u>Database Impact</u></b>	<b>9</b>
<b><u>4.</u></b>	<b><u>Infrastructure Impact</u></b>	<b>9</b>
<b><u>5.</u></b>	<b><u>Other Dependencies</u></b>	<b>9</b>
<b><u>6.</u></b>	<b><u>Security Considerations</u></b>	<b>9</b>
<b><u>7.</u></b>	<b><u>Known Issues, Limitations, and Restrictions</u></b>	<b>9</b>



{ STYLEREF Module/Acronym \\* MERGEFORMAT }

## LIST OF TABLES

<u>Table 1: Individual Application Business Capabilities</u> .....	2
<u>Table 2: My Account Business Capabilities</u> .....	4
<u>Table 3: Plan Compare Business Capabilities</u> .....	6
<u>Table 4: ESD Business Capabilities</u> .....	6
<u>Table 5: Direct Enrollment API Business Capabilities</u> .....	7
<u>Table 6: Call Center Development Business Capabilities</u> .....	7
<u>Table 7: Enrollment Business Capabilities</u> .....	8

{ STYLEREF Module/Acronym \\* MERGEFORMAT }

---

## 1. Introduction

### 1.1. Purpose

The Federally Facilitated Marketplace (FFM) Build Notes describe the key components of this build of the FFM application.

The details of the build are identified under section 1.3 and 2.1 below.

This build is to update Prod Prime with new EE and FM functionality and to correct defects since the last deployment.

### 1.2. Audience

The document is intended for users and key stakeholders of the FFM.

### 1.3. Build Manifest

**Release Name** : **Release 7.0.0.6, 7.0.0.7, 7.0.0.7.1**

**Build Number** :

**Target Platform** NotResp **Enterprise Linux**

**Target Platform Deployment Date** : **September 07, 2013**

**Deployment Schedule Artifact** :

**Deployment schedule position** : **September 07, 2013**

---

## 2. New Features and Fixed Issues

This section lists any new features, defects, or Change Requests that have been fixed and passed in this build.

### 2.1. New Features

Listed below are the new or updated features that are available in this build.

#### 2.1.1. Individual Application

In this build, enhancements were made to the individual application that enabled the following:

{ STYLEREF Module/Acronym \\* MERGEFORMAT }

- Enhancements to several eligibility determinations to handle logic for tax households, MAGI rules, and tribal status
- Trigger of Data Source Down notice when verifications return indicating that the data sources are not available
- Header/Footer updates to support help dropdown
- Capturing Agent/Broker Ids and assitor questions within the application
- Capturing ESC information in the Additional Information section
- Error Handling
  - Service errors and validations
  - Delayed response alert to consumer when DHS calls are delayed
- Updates to Person Matching service
- Triggers to support Notice generation for data sources being down
- Eligibility Determination enhancements for addressing attestations, annual/current income logic, and inconsistency clock logic

**Table 1: Individual Application Business Capabilities**

Business Capability	Feature	Task
Individual Application (Online Application)	Get Started	Get Started
		Assistor/Agent/Broker
	Additional Information	Per Person - Employer Details
		Per Person - ESC 1
		Per Person - ESC 2 (a and b)
		Per Person - Employer Contact Information
		Per Person - Select Employers
		Per Person - Select Employers Delete Modal
		Health Insurance Information for Application Members
		Medicaid and CHIP specific questions
		ESC MEC Questions
		Pre-Verification Processing Updates to Services: Income, VLP, MAGI2
	Consumer UI	UI Functionality Pages
		Header
		Footer
		Error Handling -

{ STYLEREF Module/Acronym \\* MERGEFORMAT }

		Service errors
		Error Handling - Validations
	My Account Integration	Auditing Activity
	Household Summary	FAH UI Card Flow Updates
	Eligibility Results	UI Frame - Eligibility Results
	Delayed Response	Pre-determination Processing Service
		Delayed Response Pages (2)
		Delayed / No Response
	Attestations	Modify Attestation page to check for Failed ID Proofing - UI to call Pre-Determination Service
	Building the Household & Personal Information	Person Matching
Individual Application (Elig Determination)	Manage Insurance Application and Determine Individual Eligibility	Manage Insurance Application (orchestration service)
		Create Trigger Notice service to first check if the data source down notice has already been queued on the current date and if not to insert a Processing Queue entry
	Household Composition	Household Composition - Minor Change in Service
	Determine Medicaid/CHIP Eligibility	MAGI 3 - Remove Incarceration Rule from the Logic or Hardcode to Indicate Not Incarcerated
	Determine Indian Status	Tribal Modal Updates to Display and Logic
	Determine QHP Eligibility	Update Eligibility for QHP to Address Attestations
	Predetermination processing	Changes in Current Annual Income to support Pre-verification Processing
Individual Application (Elig Results)	Start Clocks	Update Start Clock

{ STYLEREF Module/Acronym \\* MERGEFORMAT }

		Service
		Develop the Updates Needed to the Start Clock Service
		Start Clock - Income Check
	Complete eligibility	Sign and Submit Cards
Individual Application (Verification)	Verify Citizenship/Lawful Presence	Modify Citizenship/Immigration Verification to trigger the Data Source Down Notice Logic
	Verify Annual Income	Modify Annual Income Verification to Trigger the Data Source Down Notice Logic
	Verify Incarceration	Update Incarceration Verification to Address Data Element Naming Issues

### 2.1.2. My Account

In this build, enhancements were made to the My Account functionality that enabled the following:

- Integration with To-do list
- Enhancements to LOA2 step-up functionality to include screens for document upload and notification that the identify proofing is still under review.
- Enabling uses to upload documents to support inconsistency resolution
- Providing consumers the ability to invoke the appeals process
- Allowing consumers to step up their account to LOA2 and handling error conditions during that process
- CCR landing page and associated services

**Table 2: My Account Business Capabilities**

Business Capability	Feature	Task
My Account	Landing Page (Tenant): Consumer Landing Page	Bulletin Board
		Cleanup Header
		Retrieve APTC data

{ STYLEREF Module/Acronym \\* MERGEFORMAT }

	Landing Page (Global): My Apps and Coverage Global Landing Page	Cleanup Header
	Settings: My Plans & Programs	Retrieve Enrolled Plan Per Enrollment Group
		Display Plan Info
	Landing Page: Issuer	Individual Account Handling (Login)
		Keep Alive URL
		Button on App to Redirect Anytime
		Button to Redirect to Issuer with Results
	LOA2 - Online ID Proofing	ID Proofing No Attempts Left
		Step Up User - Submitter Info
		Step Up User - Modify User
		UI Validation EIDM
		Verification Status -Very Rare
		ID Proofing Attempts Left
		Step Up User - Manual Identity Proof
		EIDM Specific Error Messaging
	LOA2 - Online ID Proofing - FFM Services	Call Person Matching service for Individual App integration
		Update ID Proofing Attempts
	LOA2 - ESD Proofing	Update FARS Attempts
		Identify Still Under Review
		Upload Documents Modals
	To Do List	Document Upload Trigger ESD Task Service
		To Do List - My Account
	Settings: Inconsistencies List	Upload Document for Inconsistencies and Create ESD Tasks
		Retrieve inconsistencies (including status)
	Settings: Eligibility Results and Appeals	Retrieve Application Information
		Display Eligibility Results (Reuse individual app display or PDF)
		Associate to an appeal
		Button to send to the appeal form
	Landing Page: Agent/Broker	Landing Page

{ STYLEREF Module/Acronym \\* MERGEFORMAT }

	Landing Page: CCR	Questions Page
		Find CCR Info by ID
		Add or Update CCR Info
		Update UI to use Update CCR Info service and the find all applications service by person ID
		CCR Landing Page UI Design
		Track in Audit Trail using EMF

### 2.1.3. Plan Compare

In this build, enhancements were made to Plan Compare that enabled the following:

- Integration Security Check / State Controller: In order to ensure task are completed in sequence plan compare added Security check to make sure users finishes tasks in order.
- APTC for Anonymous: Include APTC calculations for Non Anonymous users.

**Table 3: Plan Compare Business Capabilities**

Business Capability	Feature	Task
Plan Compare	Plan Select	New Max APTC Service Integration

### 2.1.4. ESD

User Roles for Tier 1 and Tier 2 as well as the Task Management Queue View (including View All Tasks) are included in this build.

**Table 4: ESD Business Capabilities**

New Business Capability	New Feature	Task
Eligibility Support Desktop	Task Queue/Workflow	Click to View Person Details - UI
		Task Notes UI
		.XLS upload of User Roles (workaround for un-implemented Admin interface) - Services
		Notes Framework - Service
		View All Tasks - UI
		Management Task Queue View
		ESS Task Queue View (Tier 1) - UI
		ESS Management Task Queue View (Tier 2+) - UI

{ STYLEREF Module/Acronym \\* MERGEFORMAT }

		ESD Tier 1 (Scan/Mailroom and Document Task Processors)- Services
		ESD Tier 2 (Tier 1 supervisor) - Service
	Person View Verification Expansions	Person View Details Service
		ESS Worker Resolution of Verification Issues - UI
		Manager Resolution of Verification Issues - UI
	Review and Adjudication of documents submitted by consumer	ESS Worker Resolution of Verification Issues - Services
		Security -Enforce Security on Gateway Services

### 2.1.5. Direct Enrollment API

In this build, new feature has been developed to support new consumer to FFM be securely redirected from partner website to FFM.

**Table 5: Direct Enrollment API Business Capabilities**

New Business Capability	New Feature	Task
Direct Enrollment API	Secure Redirect	New Consumer Secure Redirect

### 2.1.6. Call Center Development

**Table 6: Call Center Development Business Capabilities**

New Business Capability	New Feature	Task
Call Center Development	View Authorized Representative Information	Develop Service - FFM allows CSR to view Authorized Representative Information

### 2.1.7. Enrollment

In this build, the following key features have been incorporated:

1. Inbound File Processing enhancement

- Ability for inbound 824s (new) and 834s (enhanced) to process. For 834s, benefit enrollment maintenances will be processed in chronological order. Also ensure ordering of inbound 834 files.



{ STYLEREF Module/Acronym \\* MERGEFORMAT }

## 2. Transaction logging

- Inbound 834 logging now logs the entire benefit enrollment requests.
- Inbound 999 logging now logs individual transactions.
- Inbound 824 logging now logs the original transactions.

**Table 7: Enrollment Business Capabilities**

Business Capability	Feature	Task
Enrollment	Transaction Logging - 999, 824XML, 834 (Inbound and Outbound)	Transaction Logger - Inbound 834
		Transaction Logging - Inbound 999
	Initial Enrollment	Initial Enrollment
	Change Enrollment - Cancel/Terminate Enrollment	Change Enrollment - Cancel one member from existing policy
		Change Enrollment - Terminate one member from existing policy
	Process Enrollment Service	Error Handling
	Process Inbound 834s for Effectuation, Cancellation and Termination of Enrollments from Issuers	Inbound file processing-File Splitter
		Inbound file processing-Modify Spring Batch Steps
		Inbound file processing-Data Service - (file name) (set state, check eligibility)
		Inbound file processing-Create Spring batch check eligibility
		Inbound file processing-Data service to get next round
		Inbound file processing-Define DB transaction (through service header)
		Inbound file processing-Process staging table for spring batch
		Inbound file processing-Data service - update file status
	Generate Outbound 834s for Initial, Change, Cancel, Terminate Enrollments	Outbound 834 Cancel
		Outbound 834 Terminate
		Outbound 834 Initial

### 2.1.8. Financial Management

In this build, Vendor Maintenance Manage Payee Group Page features will be available:

- Create new payee groups

{ STYLEREF Module/Acronym \\* MERGEFORMAT }

- Update existing payee groups
- Save and Continue later
- Submit For approval

## **2.2. Resolved Defects**

See accompanying spreadsheet (Prod Prime\_Build\_7.0.0.6, 7.0.0.7, 7.0.0.7.1.Defect\_Fixes.xlsx) for resolved defects.

## **2.3. System Access**

Available upon request.

---

## **3. Database Impact**

No Database Impacts.

---

## **4. Infrastructure Impact**

No infrastructure impacts.

---

## **5. Other Dependencies**

This release is dependent on EIDM and Data Service Hub services being available.

---

## **6. Security Considerations**

Refer the security documentation already submitted to CMS as part of SCA activities.

---

## **7. Known Issues, Limitations, and Restrictions**

Enrollment:

Kickoff script won't call the service. Does not prevent testing. Script can be changed in testing environment easily.

Fetch Eligibility:

- 1) We are still using old APTC Service. Need to change to use new APTC Service

{ STYLEREF Module/Acronym \\* MERGEFORMAT }

- 2) The hub partner id to issuer mapping data that we got from the hub is not latest and has many TBDs. We use this data for validation checks in Fetch Eligibility and Submit Enrollment service

#### Limitations/Restrictions:

##### Fetch Eligibility:

- 1) Waiting on POD1 changes for Snapshot Logic - Lakshmi said it will be a couple of weeks...
- 2) Autodisenrollment info at policy level - is not yet implemented per Bee (Pod2)
- 3) Earliest/Latest QHP effective dates are hardcoded - hardcoded until implemented by other pods
- 4) EnrollmentPeriod at policy level is hardcoded - hardcoded until implemented by other pods

##### Submit Enrollment:

- 1) Work still going on to switch over to new service for Submit Enrollment

##### Call Center:

Unlock Account/Reset Password service still not tested in NotResp prime by call center.

## Appointment

**From:** Broccolino, Michele (CMS/OC) NotResp

NotResp

**Sent:** 5/20/2014 4:01:21 PM

**To:** Bataille, Julie (CMS/OC) NotResp

NotResp

Reilly, Megan C. (CMS/OC) NotResp

NotResp

Liverpool, Sheila Faison (CMS/OC)

NotResp

NotResp

NotResp

Broccolino, Michele (CMS/OC) NotResp

NotResp

Booth, Jon G. (CMS/OC) NotResp

NotResp

St. Louis, Aileah (CMS/OC) NotResp

NotResp

Trefzger, William (CMS/DWO) NotResp

NotResp

Patel, Ketan (CMS/OC) NotResp

Harris, Danielle Y. (CMS/OC) NotResp

NotResp

Mitchell, Michael F. (CMS/OC) NotResp

NotResp

Ramsey, Letticia T. (CMS/OC) NotResp

NotResp

Giacomelli, Rebecca (CMS/OC) NotResp

NotResp

Pressley, Erin L. (CMS/OC) NotResp

NotResp

Miner, Amy L. (CMS/OC)

NotResp

Stoltz, Craig (CMS/OC)

NotResp

NotResp

Das, Krista (CMS/OC) NotResp

NotResp

Franklin, Julie G. (CMS/OC) NotResp

Harmatuk, Frances B. (CMS/OC) NotResp

NotResp

Johnson, Naomi E. (CMS/OC) NotResp

NotResp

Carey, Kathleen G. (CMS/OC) NotResp

NotResp

Broccolino, Mark D. (CMS/OC) NotResp

NotResp

Burdette, Jeffrey (CMS/OC) NotResp

NotResp

Judor, Susan J. (CMS/OC) NotResp

NotResp

CMS VTC NotResp

NotResp

**CC:** English, Letitia N. (CMS/OC) NotResp

NotResp

Hollman, Susan K. (CMS/OC) NotResp

NotResp

Bogley, Dennis (CMS/OC) NotResp

NotResp

Panicker, Anita G. (CMS/OC)

NotResp

Johnson, James E.

(CMS/OC) NotResp

NotResp

Burch, Mimi Z. (CMS/OC)

NotResp

**Subject:** Weekly Marketplace Consumer Tools Meeting

**Location:** OC Conference Room S1-20-01 (Baltimore) / 303D04 (DC) / Call In (b)(6) Meeting (b)(6)

**Start:** 5/21/2014 3:30:00 PM

**End:** 5/21/2014 4:00:00 PM

**Show Time As:** Tentative

**Recurrence:** Weekly

every Tuesday from 10:00 AM to 11:00 AM

**Required**

**Attendees:**

Bataille, Julie (CMS/OC); Reilly, Megan C. (CMS/OC); Liverpool, Sheila Faison (CMS/OC); Broccolino, Michele (CMS/OC); Booth, Jon G. (CMS/OC); St. Louis, Aileah (CMS/OC); Trefzger, William (CMS/DWO); Patel, Ketan (CMS/OC); Harris, Danielle Y. (CMS/OC); Mitchell, Michael F. (CMS/OC); Ramsey, Letticia T. (CMS/OC); Giacomelli, Rebecca (CMS/OC); Pressley, Erin L. (CMS/OC); Miner, Amy L. (CMS/OC); Stoltz, Craig (CMS/OC); Das, Krista (CMS/OC); Franklin, Julie G. (CMS/OC); Harmatuk, Frances R. (CMS/OC); Johnson, Naomi E. (CMS/OC); Carey, Kathleen G. (CMS/OC); Broccolino, Mark D. (CMS/OC); Burdette, Jeffrey (CMS/OC); Tudor, Susan J. (CMS/OC); CMS VTC

**Marketplace Consumer Tools Meeting Agenda**

1. Consumer Tools Updates and PMR Dashboard Review (see document attached) – Megan Reilly and Jon Booth
2. Sub-Tower Updates
  - i. My Account – Susan Tudor
  - ii. Account Creation & Authentication – Ketan Patel  
(NOTE: Need SLS update for this week's Priorities Meeting)
  - iii. Application – NOTE: Michael Mitchell will do an app update in the Application 2.0 Follow-up Meeting (Wednesday, May 21<sup>st</sup> at 12:00pm)
  - iv. Plan Compare – Letticia Ramsey
  - v. Learn Side and Global HCare.gov – Craig Stoltz & Aileah St. Louis



OC Dashboard  
Consumer Tools ...

+-----+-----+-----+-----+-----+-----+-----+-----+

[Do not add or change anything below this line. The information in this section may be replaced with your meeting details after you click Send.]

You scheduled this meeting.

Meeting Number: (b)(6)

Meeting Password: This meeting does not require a password.

-----  
**Audio conference information**  
-----

1. Please call the following number:

WebEx: (b)(6)

2. Follow the instructions you hear on the phone.

Your WebEx Meeting Number: (b)(6)

-----  
To join from a Cisco VoIP enabled CMS Region or from CMS Central Office  
-----

1. Dial ext (b)(6)

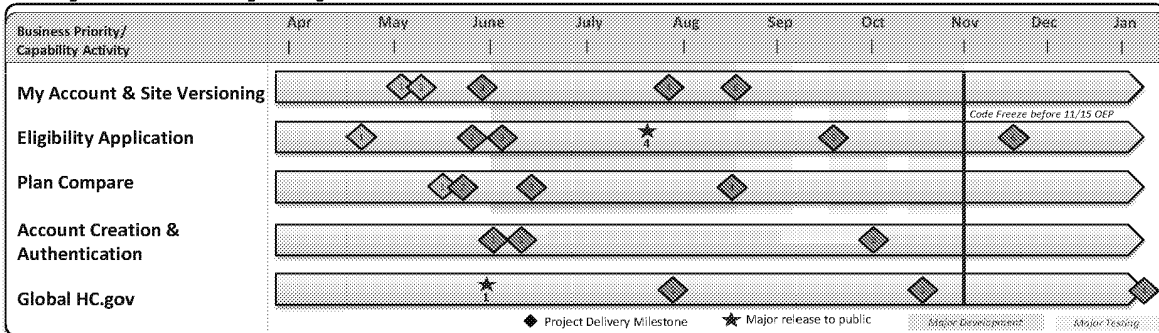
2. Enter the Meeting Number (b)(6)

-----  
To start the online meeting

-----  
1. Go to https:// (b)(6)

2. If you are not logged in, log in to your account.

# Key Priority Update: Consumer Tools - Highlights



#	My Account & 2015 Site Versioning	Plan	Actual
1	Draft consumer scenarios for user pathways through the site for 2014 & 2015 consumer activities	5/6	5/6
2	Draft conceptual wireframes for FFM Landing Page changes to support 2014 & 2015 consumer activities	5/9	5/9
3	Solidify Landing Page requirements, My Account requirements & basic 2015 versioning changes needed	5/30	
4	Complete development for 2015 versioning	7/25	
5	Testing Begins	8/15	

#	Eligibility Application	Plan	Actual
1	Ongoing CMS SME testing of Marketplace (MP) Application 2.0	Mid Apr – Mid June	
2	ATO issued for MP Application 2.0	5/23	
3	Finalize 2014 to 2015 logic for application copy/versioning to support consumers with an existing '14 application	6/6	
4	Go/No-Go & Initial public launch of Application 2.0 to 1% traffic	7/18	
5	Integrated In-depth ACA, UAT & Issuer Testing of Application 2.0 & FFM Classic Application with 2015 rules (round 2, round 3)	9/12 – 10/10 10/3 – 10/31	
6	Publish revised paper application	11/15	

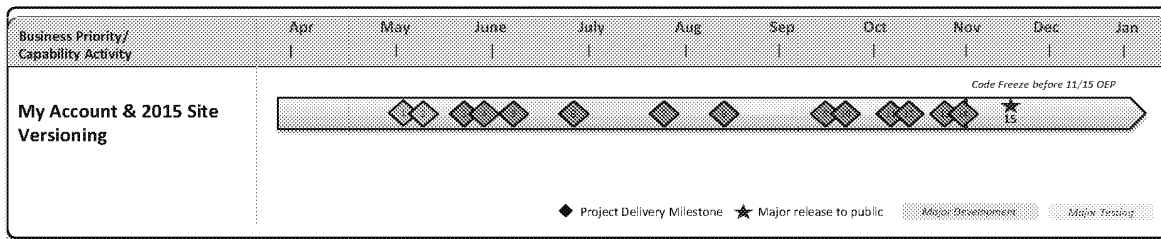
#	Plan Compare	Plan	Actual
1	Draft strategy for development integration for system flows across FFM & PC 2.0 elements	5/16	5/16
2	Finalize development contract mod for Plan Compare 2.0	5/20	
3	Complete business requirements for 2015 versioning	6/6	
4	FFM & MP 2.0 PC Development Complete – Conduct Integrated ACA, UAT, & Issuer testing using test data	8/15	

#	Account Creation & Authentication	Plan	Actual
1	Test migration strategy from EIDM to SLS	End of May	
2	Finalize strategy for Log In pathways for consumers vs. SHOP employer & employee accounts (FFM)	Late May – Early June	
3	Launch SLS – Production migration of consumer accounts	October 1	

#	Global HC.gov Changes	Plan	Actual
1	Non OEP Screener launch & Homepage changes – New Calls to Action (Screener, SHOP)	5/30	
2	Find Local Help – update data collection tool & enhance data & UX for improved consumer content	TBD Late Summer	
3	OEP Content & Information Architecture Changes	October	
4	Consumer Tax Tools	January	



# Key Priority Update: Consumer Tools – My Account & 2015 Site Versioning

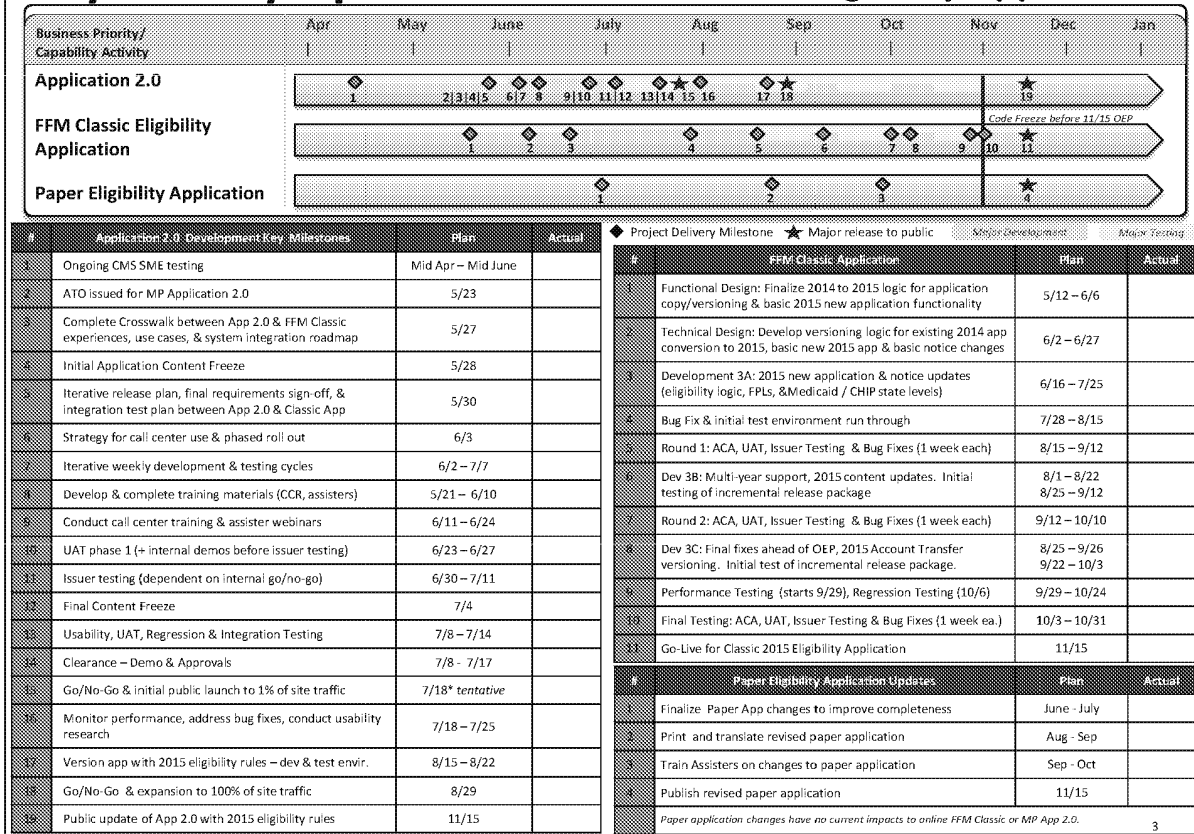


#	My Account & 2015 Site Versioning Key Milestones	Plan	Actual
1	Draft consumer scenarios for user pathways through the site for 2014 & 2015 consumer activities	5/6	5/6
2	Draft conceptual wireframes for FFM Landing Page changes to support 2014 & 2015 consumer activities	5/9	5/9
3	Inventory of changes & types of versioning needed by section within My Account	5/23	
4	Solidify Landing Page requirements, My Account requirements & basic 2015 versioning changes needed	5/30	
5	Functional Design Complete: My Account, Landing Page, web services for support channels 2015 versioning requirements finalized	6/6	
6	Technical Design Complete: 2015 basic consumer scenario through My Account & 2015 site versioning	6/27	
7	Development 3A: 2015 changes for Landing Page, My Account, overall FFM site versioning, updated call center web services	6/16 – 7/25	
8	Bug Fix & Initial test environment run through	7/28 – 8/15	
9	Round 1: ACA, UAT, Issuer Testing & Bug Fixes (1 week each)	8/15 – 9/12	
10	Dev 3B: Multi-year support, 2015 content updates. Initial testing of incremental release package	8/1 – 8/22   8/25 – 9/12	
11	Round 2: ACA, UAT, Issuer Testing & Bug Fixes (1 week each)	9/12 – 10/10	
12	Dev 3C: Final fixes ahead of OEP, 2015 Account Transfer & Direct Enrollment versioning. Initial test of incremental release package.	8/25 – 9/26   9/22 – 10/3	
13	Performance Testing (starts 9/29), Regression Testing (10/6)	9/29 – 10/24	
14	Final Testing: ACA, UAT, Issuer Testing & Bug Fixes (1 week ea.)	10/3 – 10/31	
15	Consumer Go-Live in production	11/15	

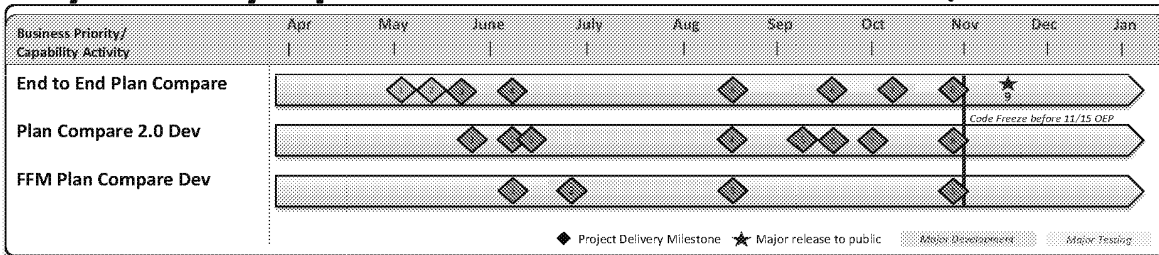




# Key Priority Update: Consumer Tools – Eligibility Application



# Key Priority Update: Consumer Tools – Plan Compare



#	End-to-End Plan Compare Milestones	Plan	Actual
1	Draft consumer flows for major consumer scenarios	5/6	5/6
2	Draft strategy for development integration for system flows across FFM & PC 2.0 elements	5/16	5/16
3	Kick off Plan Compare integration with PC 2.0 & FFM development teams	5/19 - 5/23	
4	Finalize development requirements between FFM & Plan Compare 2.0 system components (functional design complete)	6/6	
5	3A Testing: Integrated ACA, UAT, & Issuer testing using test/dummy data (1 week each, 4 <sup>th</sup> week is bug fix)	8/15 - 9/12	
6	3B Testing: In-depth ACA, UAT & Issuer testing with draft 2015 QHP data (1 week each, 4 <sup>th</sup> week is bug fix)	9/12 - 10/10	
7	3C Testing: Final ACA, UAT & Issuer Testing (1 week each, 4 <sup>th</sup> week is bug fix)	10/3 - 10/31	
8	Update production package with final, locked down QHP data	10/22 - 11/7	
9	Consumer Go-Live in production	11/15	

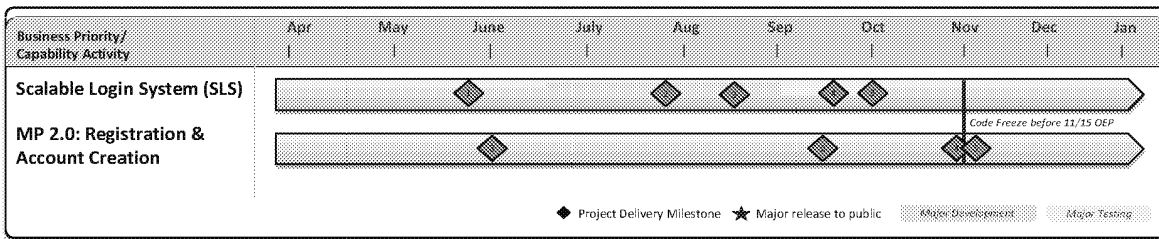
#	FFM Plan Compare Development Key Milestones	Plan	Actual
1	Draft 2015 changes needed to business logic for Enroll To-Do List, To-Do List Tasks, & backend services	6/6	
2	Complete technical requirements for 2015 versioning	6/27	
3	Initial development complete for 2015 plan compare	8/15	
4	Initial cut of draft 2015 QHP data	9/8	
5	Final cut of 2015 QHP data	10/21 - 11/4	

QHP data cuts dependent on PM milestones (ranges account for internal plan vs. public dates)

#	Plan Compare 2.0 Development Key Milestones	Plan	Actual
1	Finalize development contract mod	5/20	
2	Complete business requirements for PC 2.0 QHP data store	Early June	
3	Complete business requirements for PC 2.0 UI/UX	Early June	
4	Initial development complete	8/15	
5	Load initial draft 2015 QHP data	9/9 - 9/12	
6	Security Control Audit (SCA)	Mid-Sept	
7	ATO issued	10/1	
8	Load final 2015 QHP data	10/22 - 11/7	



# Key Priority Update: Consumer Tools – Account Creation & Authentication



#	SLS Milestones	Plan	Actual
1	Test migration strategy from EIDM	End of May	
2	Initial development complete	End of July	
3	Security Control Audit (SCA)	Mid-Aug	
4	ATO issued	Mid-Sept	
5	Launch (production migration)	October 1	

NOTE: dates are conservative and will be refined with dev team input over the next 2 weeks

#	Registration & Account Creation Milestones	Plan	Actual
	MP 2.0 – launched new account creation screens	Feb	Feb
1	MP 2.0 - 100% cutover for account creation screens from FFM to MP 2.0 Registration	TBD	
2	Finalize strategy for Log In pathways for consumers vs. SHOP employer & employee accounts	Late May – Early June	
3	FFM – Update Login page on HC.gov to include user role selection in test environments (consumer, employer, employee) – tentative pending strategy	Sept	
4	MP 2.0 - Update Account Creation to include SHOP Employer and SHOP Employee accounts ** (integrated with SHOP tower)	Oct - Nov	
5	FFM – release updated Log In strategy for multiple roles (consumer, employer, employee)	Oct - Nov	

## STATUS UPDATE

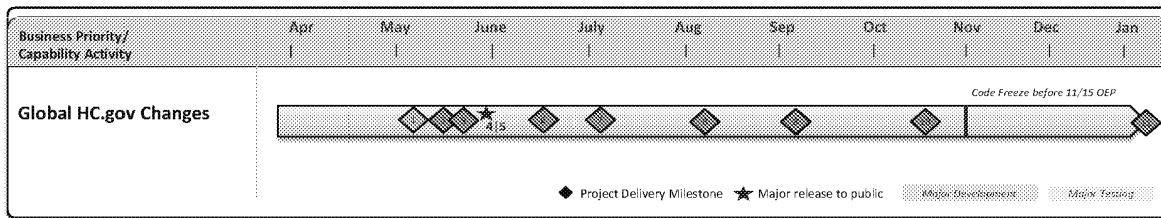
- 5/16 Conducted cross-functional offsite on SLS Implementation Planning to dive into high level design discussions, identify business requirement needs, order of steps towards implementation, decisions or strategies that need to be finalized, & begin a deeper dive on technical architecture & system flows from current state (EIDM, FFM, RIDP) to future state (SLS, FFM, RIDP)
- Drafting systems inventory with key points of contact & high level timeline including major milestones & migration points
- Identifying required clearances, technical reviews, and any outstanding technical documentation requirements
- Identified data dependencies for final migration approach/options

## Upcoming Decision Points

- RIDP Integration Strategy (Business Decision) – SLS direct connection to RIDP or SLS integration with HUB to RIDP
- EIDM Account Migration Strategy – likely will require direct assistance in the next few weeks to assist in approach & actual migration
- Finalize SHOP integration between FFM, SLS, EIDM & how the user flow gets from the front end of HC.gov through account creation & log in to SHOP product for employers & employees. Dependency: SHOP follow up conversation with IT resources, business owners & system owners

**NotResp**

# Key Priority Update: Consumer Tools – Global HC.gov



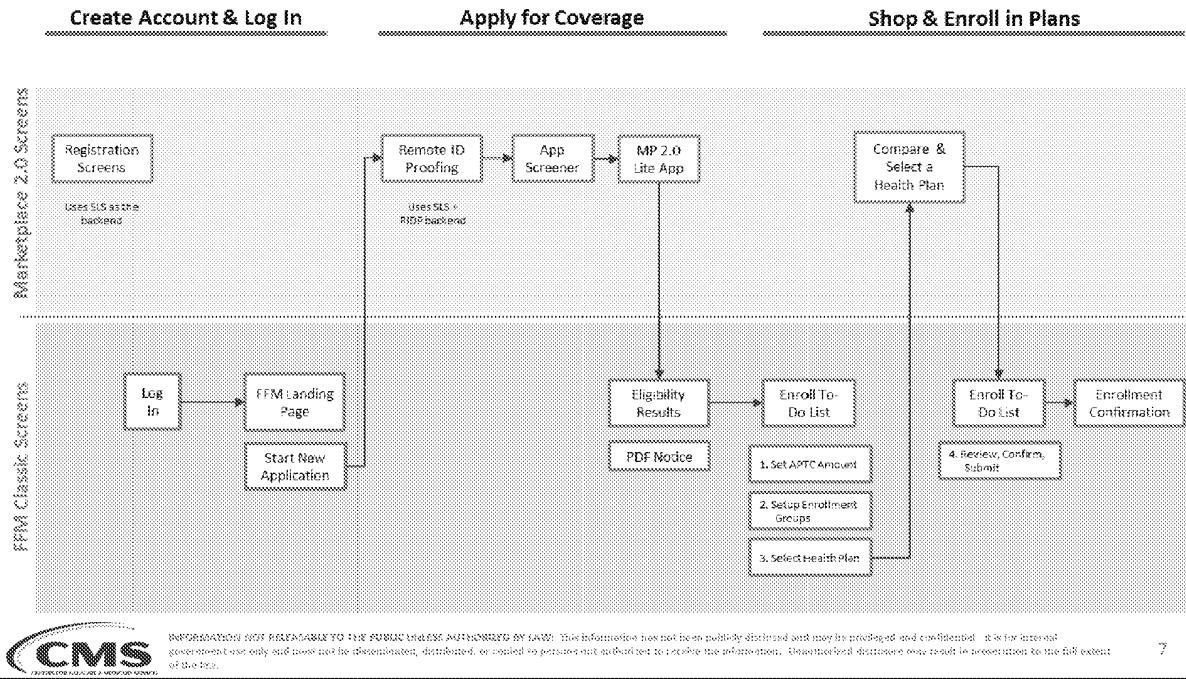
#	Global HC.gov Milestones	Plan	Actual
1	Draft consumer scenarios for user pathways through the site for 2014 & 2015 consumer activities	5/6	5/6
2	Non OEP Coverage Screener Tool Clearance Begins	Clearance Begins 5/14	[TBD: final clearance date]
3	Finalize visual refresh for Marketplace 2.0 look & feel	Late May – Early June	
4	Launch Non OEP Coverage Screener Tool	5/30	
5	Launch Healthcare.gov Homepage changes (new headline for screener, primary CTA changes to screener, secondary CTA changes to SHOP small business tools)	5/30	
6	Draft strategy for OEP information architecture to account for new consumer pathways & activities	Early – Mid June	
7	Launch HC.gov visual refresh for MP 2.0 (dependency: Application 2.0 launch)	Late June – Early July	
8	Find Local Help updates for data collection tool & improved consumer content	TBD Late Summer	
9	Develop content changes across site (consolidate, archive, reorganize, expand, new content for new consumer scenarios)	July - September	
10	Launch HC.gov OEP changes (new calls to action, updated information architecture, content revisions, etc)	October	
11	Consumer tax tools go-live	Late January	



## Consumer Experience – Simple Case

Demonstrates the simplest case of a brand new user who is creating an account, applying and enrolling all in one sitting. There are additional steps in the process and parts of the site that the consumer would interact with to complete the application and enrollment process based on their situation

The flow below shows the interaction between Marketplace 2.0 and the FFM classic systems.



Message

**From:** Fryer, Teresa M. [NotResp]  
[NotResp]  
**Sent:** 5/2/2014 3:35:11 PM  
**To:** Booth, Jon G. (CMS/OC) [NotResp]  
Marantan, James (CMS/OIS) [NotResp]  
**CC:** Chao, Henry (CMS/OIS) [NotResp] Bailey,  
Michele (CMS/OIS) [NotResp]  
**Subject:** RE: Discussion of EIDM Migration

Hi Jon,

Sure thing, Mondays are usually light and Tuesday afternoon is okay. Please work with Michele Bailey to schedule some time.

Thanks!

Teresa

**From:** Booth, Jon G. (CMS/OC)  
**Sent:** Friday, May 02, 2014 11:33 AM  
**To:** Fryer, Teresa M. (CMS/OIS); Marantan, James (CMS/OIS)  
**Cc:** Chao, Henry (CMS/OIS)  
**Subject:** Discussion of EIDM Migration

Teresa & James,

I wanted to see if we could grab some time early next week to discuss the new consumer account system we've been tasked with building for HealthCare.gov (Scalable Login System)?

Before we proceed, I'd like to discuss some of the repercussions of this migration so that we can make sure the architecture and migration strategy are acceptable from a security perspective.

Thanks,

Jon

Message

**From:** Fryer, Teresa M. [NotResp]  
[NotResp]  
**Sent:** 5/2/2014 3:37:05 PM  
**To:** Chao, Henry (CMS/OIS) [NotResp] Booth, Jon  
G. (CMS/OC) [NotResp] Marantan,  
James (CMS/OIS) [NotResp]  
**CC:** Bailey, Michele (CMS/OIS) [NotResp]  
Linares, George E. (CMS/OIS) [NotResp]  
[NotResp] Berkley, Katrina (CMS/OIS) [NotResp]  
[NotResp]  
**Subject:** RE: Discussion of EIDM Migration

Yes, thanks!

**From:** Chao, Henry (CMS/OIS)  
**Sent:** Friday, May 02, 2014 11:37 AM  
**To:** Fryer, Teresa M. (CMS/OIS); Booth, Jon G. (CMS/OC); Marantan, James (CMS/OIS)  
**Cc:** Bailey, Michele (CMS/OIS); Linares, George E. (CMS/OIS); Berkley, Katrina (CMS/OIS)  
**Subject:** RE: Discussion of EIDM Migration

Would be good to include George.

Henry Chao  
Deputy CIO & Deputy Director,  
Office of Information Services  
Centers for Medicare & Medicaid Services  
410-786-1800

**From:** Fryer, Teresa M. (CMS/OIS)  
**Sent:** Friday, May 02, 2014 11:35 AM  
**To:** Booth, Jon G. (CMS/OC); Marantan, James (CMS/OIS)  
**Cc:** Chao, Henry (CMS/OIS); Bailey, Michele (CMS/OIS)  
**Subject:** RE: Discussion of EIDM Migration

Hi Jon,

Sure thing, Mondays are usually light and Tuesday afternoon is okay. Please work with Michele Bailey to schedule some time.

Thanks!

Teresa

**From:** Booth, Jon G. (CMS/OC)  
**Sent:** Friday, May 02, 2014 11:33 AM  
**To:** Fryer, Teresa M. (CMS/OIS); Marantan, James (CMS/OIS)

**Cc:** Chao, Henry (CMS/OIS)

**Subject:** Discussion of EIDM Migration

Teresa & James,

I wanted to see if we could grab some time early next week to discuss the new consumer account system we've been tasked with building for HealthCare.gov (Scalable Login System)?

Before we proceed, I'd like to discuss some of the repercussions of this migration so that we can make sure the architecture and migration strategy are acceptable from a security perspective.

Thanks,

Jon



Message

**From:** Schankweiler, Thomas W. (CMS/OIS) [NotResp]  
[NotResp]  
**Sent:** 12/13/2012 9:28:40 PM  
**To:** Miller, Daniel J. [NotResp]  
Hung B. (CMS/OIS) [NotResp]  
[NotResp] Dunick, Walter T. (CMS/OIS) [NotResp]  
[NotResp]  
[NotResp] Alvarez,  
Carlos (CMS/OIS) [NotResp]  
[NotResp]  
[NotResp] Schmidt,  
Donna W. (CMS/OIS) [NotResp]  
Jenkins, Michelle L. (CMS/OIS) [NotResp]  
[NotResp]  
**CC:** Thompson, Tyrone (CMS/OIS) [NotResp]  
[NotResp]  
[NotResp]  
**Subject:** [NotResp]  
**Importance:** High

**From:** Miller, Daniel J. (CMS/OIS)  
**Sent:** Thursday, December 13, 2012 3:42 PM  
**To:** Van, Hung B. (CMS/OIS); Dunick, Walter T. (CMS/OIS); Chao, Bing (CMS/OIS); Alvarez, Carlos (CMS/OIS); Lelis, Nikoleta (CMS/OIS); Schankweiler, Thomas W. (CMS/OIS); Schmidt, Donna W. (CMS/OIS); Jenkins, Michelle L. (CMS/OIS)  
**Cc:** Thompson, Tyrone (CMS/OIS); Nguyen, Tina D. (CMS/OIS)  
**Subject:** Action Needed: Project Status (1-2 Sentences from Each of You)  
**Importance:** High

Hi IT PM's, need your help to pull some quick information for Monique and Tina who need to package some reports for leadership. Can each of you copied provide one to two sentences that describes the current individual status for your respective project as outlined below? Along with an estimated green/yellow/red status? Tyrone and Mark will govern this, but we have a fire drill where we need to put this together in the next couple hours. See the first row as an example:

Project	Owner	St a t u s  C o l o r  (	Description (1-2 sentences describing overall status)
		G	

		r e e n, Y e l l o w , R e d)	
FFE- Plan Manag ement	Carlos Alvarez	Y e l l o w	Few to no changes can be accommodated without jeopardizing the 3/28/2013 <b>NotResp</b> data collection go-live date.
FFE- Financi al Manag ement	Walt Dunick		
FFE- Eligibilit y and Enrollm ent	Hung Van/Bin g Chao		
Data Service s Hub	Hung Van/Bin g Chao		
State Integrat ion	Niki Lelis		
MIDAS	Glenn Radcliffe /Michell e Jenkins		
Securit y Cloud Monito ring	Tom Schankw eiler	Y e l l o w	Experiencing difficulty with <b>NotResp</b> in regards to their prioritization of work activity to have setup proper network paths to allow traffic to reach the monitors. Part of this is CMS imposed delay's due to a heavy work volume being placed on the vendor. <b>NotResp</b>
Securit y Cloud Testing	Tom Schankw eiler	G r e e	<b>NotResp</b>

		n	
Security ISA	Tom Schankweiler	Green	On Schedule

Donna and Michelle J: With Glenn's great baby news, could you provide a one-liner for MIDAS? (Guessing it's green.)

[And Donna if Niki is out of commission, maybe a one-liner on State integration?]

Tom: If you want to propose a single status for Security overall, that's probably OK for this one. (But I kept it broke out as three rows just in case.)

Thanks if you guys can get that back to us by 5:30 p.m. tonight!

**Daniel J. Miller**

Deputy Director, Division of Application and Data Services (DADS)

Consumer Information & Insurance Systems Group (CIISG)

Office of Information Services (OIS) - Centers for Medicare & Medicaid Services (CMS)

U.S. Department of Health & Human Services (DHHS)

Mobile Phone (bb): (b)(6) Office Phone: (301) 492-4364

[daniel.miller2@cms.hhs.gov](mailto:daniel.miller2@cms.hhs.gov) | [www.healthcare.gov](http://www.healthcare.gov)

**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.

Message

**From:** Schankweiler, Thomas W. (CMS/OIS) [NotResp]  
[NotResp]  
**Sent:** 4/24/2012 5:39:26 PM  
**To:** Miller, Daniel J. (CMS/OIS) [NotResp]  
James, Brian M. (CMS/CCIIO) [NotResp]  
Shropshire, Richard (CMS/CCIIO) [NotResp]  
[NotResp] Lyles, Darrin V. (CMS/OIS) [NotResp]  
[NotResp]  
Goswami, Mayank (CGI Federal) [Mayank.Goswami@cgifederal.com]; Johar, Sandeep S (CGI Federal) [sandeep.johar@cgifederal.com]  
**CC:** Brackett, Stacie D. (CMS/CPC) [NotResp]  
[NotResp] Cummings, Duane (CGI Federal) [Duane.Cummings@cgifederal.com]; Welshans, Richard (CGI Federal) [Richard.H.Welshans@cgifederal.com]; Ramamoorthy, Balaji Manikandan (CGI Federal) [balajimanikandan.ramamoorthy@cgifederal.com]; Rashid, Musharaf U (CGI Federal) [musharaf.rashid@cgifederal.com]  
**Subject:** RE: Security & Two-Factor Authentication for HIOS/FFE

Brian, here is the strategy for bringing EHB system on-line.

1. Submit the Core Impact form and establish the system in CFACTS
2. Identify Cfacts data entry person (contractor) begin establishing access and training.
3. Generate a FIPS-199, and a PTA/PIA document in CFACTS
4. Servers are built from baseline virtual images (CM)
5. Test servers and databases using Nessus and Mitre Scripts, (results to be provided to Mitre for review and feedback)
6. Document weakness in a spreadsheet, and take initial steps to resolve issues
7. Integrate new system into management and security tools sets
8. Create a draft SSP which documents control for hybrid and system specific controls
9. Create an initial Risk Assessment document
10. Schedule a formal ST&E

-----Original Appointment-----

**From:** Miller, Daniel J. (CMS/OIS)  
**Sent:** Thursday, April 19, 2012 10:07 AM  
**To:** Miller, Daniel J. (CMS/OIS); Schankweiler, Thomas W. (CMS/OIS); James, Brian M. (CMS/CCIIO); Shropshire, Richard (CMS/CCIIO); Lyles, Darrin V. (CMS/OIS); Goswami, Mayank (CGI Federal); Johar, Sandeep S (CGI Federal)  
**Cc:** Brackett, Stacie D. (CMS/CPC); Cummings, Duane (CGI Federal); Welshans, Richard (CGI Federal); Ramamoorthy, Balaji Manikandan (CGI Federal); Rashid, Musharaf U (CGI Federal)  
**Subject:** Security & Two-Factor Authentication for HIOS/FFE  
**When:** Tuesday, April 24, 2012 1:00 PM-2:00 PM (GMT-05:00) Eastern Time (US & Canada).  
**Where:** Dial-In [ (b)(6) ] or Meet in 9th Floor CIISG Conference Room in Bethesda

When: Tuesday, April 24, 2012 1:00 PM-2:00 PM (GMT-05:00) Eastern Time (US & Canada).

Where: Dial-In (b)(6) or Meet in 9th Floor CIISG Conference Room in Bethesda

Note: The GMT offset above does not reflect daylight saving time adjustments.

\*~\*~\*~\*~\*~\*~\*~\*~\*~\*

Hi all, I'm updating this invite with the dial-in and a description of the 4 specific issues we want to discuss:

**Dial-In:** (b)(6)

**Physical Location:** 9<sup>th</sup> Floor CIISG Conference Room (for those of us in Bethesda)

Issues: Here are the 4 items we want to discuss:

- **Security Between Now and July 1 to Enable EHB State Benchmark Data Collection:** On July 1, one user per each State, and three Issuers per each State, will begin submitting a finite set of data (EHB State Benchmark) to FFE Plan Management, and will be authenticated through the existing HIOS legacy system. (Most, if not all, are existing users of HIOS.) Are there any security issues/items that must be addressed by either the FFE side of the house (Mayank's team) and/or the HIOS Legacy side of the house (Brian's team?) Although this is a small sliver of data being collected (in compared to the "Go Live" system collection for the QHP Issuer Data Collection described below in January 2013) want to make sure we're not missing anything.
- **Timing of MFA:** For both FFE and HIOS Legacy, when is multi-factor authentication required to be implemented? If it isn't absolutely required for the July EHB collection date, what timeframe will it make pragmatic sense to implement? After July 1, milestones on the FFE side are:
  - October 1, 2012: All Issuer data collection and evaluation features will have been internally built out and ready for training with external testers, more comprehensive end-to-end system integrated testing, etc.
  - December 1, 2012: Issuers in each FFE State will submit "NOI" data into the FFE system, authenticated through HIOS Legacy, a very small subset of data.
  - January 1, 2013: Issuers in each FFE State will submit the QHP Issuer Application, a complex set of data, documents and Excel templates to the FFE system. This is the date we think of as the true "Go Live" production date for the FFE Plan Management System.
  - February 15, 2013: Issuers in each FFE State will submit the Rate and Benefit Data Submission, a "part 2" complex set of data, documents and Excel templates to the FFE system. (But from a system security standpoint don't imagine anything that must be ready by this date that shouldn't have already happened by January 1, 2013.)
- **MFA vs. TFA vs. PFA:** Brian's HIOS Legacy team had purchased Phone-Factor based on prior instruction but sounds like that might be contradictory to using the Sysmantec Multi-Factor Authentication product. What do we need to reconcile?
- **LDAP:** To what extent do our plans of integrating with CMS LDAP affect any of the above?

See you all then.

**Daniel J. Miller**

Deputy Director, Division of Application and Data Services (DADS)

Consumer Information & Insurance Systems Group (CIISG)

Office of Information Services (OIS) - Centers for Medicare & Medicaid Services (CMS)

U.S. Department of Health & Human Services (DHHS)

Mobile Phone (bb): (b)(6) Office Phone: (301) 492-4364

daniel.miller2@cms.hhs.gov | [www.healthcare.gov](http://www.healthcare.gov)

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.

**Blank Page**

Message

**From:** Schankweiler, Thomas W. (CMS/OIS) [NotResp]  
[NotResp]  
**Sent:** 6/1/2012 9:26:15 PM  
**To:** Cooper, Dennis (CMS/CTR) [NotResp]  
[NotResp] 'Kris Blais' [kblais@spherecomenterprises.com]  
**Subject:** FW: FW: CCIO: Upcoming Travel Discussion

FYI

---

**From:** Miller, Daniel J. (CMS/OIS)  
**Sent:** Friday, June 01, 2012 1:07 PM  
**To:** Schankweiler, Thomas W. (CMS/OIS)  
**Cc:** Oh, Mark U. (CMS/OIS)  
**Subject:** RE: FW: CCIO: Upcoming Travel Discussion

Sure Tom. Here is what it will be:

**Location:** NAIC Headquarters located at:  
1100 Walnut Street  
Suite 1500  
Kansas City, MO 64106-2197

**Duration:** 1.5 Days

**Purpose and Scope:** Meet with NAIC's technical team and lead security manager, and and perform a high-level assessment to gain an understanding of the system and security in place in order to perform a summary gap analysis between NIST-3 and other federal standards required in order to enable Exchange States to use SERFF to perform Plan Management QHP functions including data collection and (potentially) analysis, including transmission of final data to FFE for display on the portal to consumers. This initial meeting would inform CMS at a broad perspective what NAIC might need to change/mitigate and/or for CMS to assume from a risk perspective to move forward. The purpose is not to finalize, in this initial meeting, the exact findings, but rather give CMS an overall perspective for how many security resources and work we might need to provide to NAIC to help meet the standards, including the completion of security documentation, analysis of findings, etc. It is important to understand the overall mission is to not let NAIC fail in meeting security standards, which is a critical item for us to ensure a successful model for Exchange State Parntners, and thus to help us determine how to get there. Our team should understand there is some (natural) sensitivity from the NAIC team in exposing their overall system to us, and we have been careful to explain to them our good faith intentions in using this analysis to ultimate make sure our partnership regarding the Exchanges works (and not as a hammer to shut them out of participating in the Exchanges). In the Monday meeting Mark Oh can correct me and/or add to this in terms of the objectives if different than what I've stated here.

**Date:** TBD, but likely as early as within the next 1-3 weeks. Date hinges NAIC's management approving this decision; our immediate contacts have already bought into this concept, and are selling this to the NAIC excutives and Security Director who may be slightly apprehensive that we would use this to expose security risks and/or impose undue/expensive burden on them.

**Key Persons Involved from NAIC:**

- Bridget Kieras, NAIC SERFF's Product Support Manager and SERFF HIX Project Manager and day to day liaison to the NAIC development/architecture/technical team including the two individuals below

(Bridget, Steve and Joy are the typical 3 individuals on most technical discussions with us)

- Steve Anderson, NAIC Lead Architect
- Joy Morrison, SERFF Assistant Director
- Julie Fritz, NAIC's Chief Business Strategy and Development Officer and the ultimate head of all things NAIC regarding our partnership
- Kim Chrisman, SERFF Manager Product Development
- NAIC Security head to be named. NAIC also has a third-party security consultant team who may be trying to sway them around some of these issues.

Talk to you Monday.

**Daniel J. Miller**

Deputy Director, Division of Application and Data Services (DADS)

Consumer Information & Insurance Systems Group (CIISG)

Office of Information Services (OIS) - Centers for Medicare & Medicaid Services (CMS)

U.S. Department of Health & Human Services (DHHS)

Mobile Phone (bb): (b)(6) Office Phone: (301) 492-4364

[daniel.miller2@cms.hhs.gov](mailto:daniel.miller2@cms.hhs.gov) | [www.healthcare.gov](http://www.healthcare.gov)

**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:** Schankweiler, Thomas W. (CMS/OIS)

**Sent:** Friday, June 01, 2012 12:43 PM

**To:** Miller, Daniel J. (CMS/OIS)

**Subject:** RE: FW: CCIIO: Upcoming Travel Discussion

If you have any preliminary details you can share that would be great. Place, Time, duration of site visit, scope, etc...

-----Original Appointment-----

**From:** Miller, Daniel J. (CMS/OIS)

**Sent:** Friday, June 01, 2012 10:22 AM

**To:** Schankweiler, Thomas W. (CMS/OIS); Blais, Kris M. (CMS/CTR); Oh, Mark U. (CMS/OIS); Cooper, Dennis (CMS/CTR); bhjackson@spherecomenterprises.com; Warren, Kevin (CMS/OIS); Lyles, Darrin V. (CMS/OIS); kblais@spherecomenterprises.com; dcooper@spherecomenterprises.com

**Subject:** Accepted: FW: CCIIO: Upcoming Travel Discussion

**When:** Monday, June 04, 2012 2:00 PM-2:30 PM (GMT-05:00) Eastern Time (US & Canada).

**Where:** Teleconference

Sure Tom, I can join that meeting. In fact I just got off the phone with Julie Fritz at the NAIC who is meeting with our IT Security Director and mgt leadership early next week to get this approved and scheduled. See you guys Monday.



Message

**From:** Schankweiler, Thomas W. [NotResp]  
 [NotResp]  
 on behalf of Schankweiler, Thomas W. (CMS/OIS)  
**Sent:** 10/16/2012 4:24:53 PM  
**To:** SHEPHERD, David [DSHEPHERD@lmi.org]  
**CC:** Oh, Mark U. (CMS/OIS); [NotResp]  
 [NotResp]; 'NABORS, Alan' [anabors@lmi.org]; Miller, Daniel J. (CMS/OIS)  
 [NotResp]; Lyles, Darrin V. (CMS/OIS)  
 (Darrin.Lyles@cms.hhs.gov); [NotResp]  
 [NotResp]  
**Subject:** RE: extract mtg Th 4-5?

David,

You can download all of the templates from the link below. I will also need to provide you with an encrypted copy of the CMS Technical Reference Architecture (TRA) guidance and supplements.

<http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html>

you will need to download the following:

- ARS Appendix B CMSR Moderate Impact Level Data v 1.5
- ARS Appendix D CMSR e-Authentication Standard v1.5
- Authorization To Operate Package Guide v3.0
- CMS Information Security Risk Acceptance Template v1.2
- CP Procedure v 1.0
- CP Template v1.0
- CP Test Template for Tabletop Tests 1.1
- Incident Handling Procedures v2.3
- Incident Handling Template
- Information Security Agreement Template v1.0
- Minimum Security Configuration Standards for OS
- Policy for Desktop-Laptop Resources
- Policy for Information Security
- Policy for the Information Security Program
- Risk Assessment Procedure v1.0
- Risk Assessment Template v3.1
- RMH Vol 1 Chapter 10 CMS Risk Management Terms, Definitions, and Acronyms
- RMH Vol II Procedure 1-1 Accessing CFACTS
- RMH Vol II Procedures 2-3 Categorizing an Information System
- RMH Vol II Procedures 4-2 Documenting Security Controls in CFACTS
- RMH Vol II Procedures 5-6 Documenting Security Control Effectiveness in CFACTS
- RMH Vol II Procedures 6-2 POA&M Management
- RMH Vol II Procedures 6-3 Security Information Review
- RMH Vol III Standard 3-1 Authentication
- ROB for Connection to CMS
- Security CBT

- Security Certification Form template v2.0
- SSP Procedures v1.1
- SSP Template v3.1
- SSP Workbook App E level 2 e-Authentication
- SSP Workbook Main v1.5
- System Security levels by Information Type 4.0
- Test Scripts App B Moderate Level Data Assessments
- Test Scripts Main
- Tool: System Categorization Worksheet

Also do you currently have a CMS user ID? You will need to request a User Access Request form from Dan Miller so that you can get access to the CMS contractor network and a CMS e-mail address so that you can access CFACTS. Once you have access to CFACTS you will have to attend a two hour training class on using that tool. CFACTS is the application where you store all of your security documentation and artifacts. Also when you receive your CMS account they will require you to complete annual CMS security based training via CBT format.

Look forward to working with you.

Tom Schankweiler, CISSP  
Information Security Officer, CCIIO  
CMS\OIS\CIISG  
Consumer Information and Insurance Systems Group  
410-786-5956 (Balt. Office, N2-13-22)  
(b)(6) (Mobile)

**From:** NABORS, Alan [mailto:anabors@lmi.org]  
**Sent:** Tuesday, October 16, 2012 11:45 AM  
**To:** Miller, Daniel J. (CMS/OIS); Zdanowicz, Gina M. (CMS/CCIIO); O'KEIFF, Jim; OWEN, Whitney  
**Cc:** Parish, Elizabeth E. (CMS/CCIIO); Muoneke, Evonne N. (CMS/CCIIO); Davis, Natalie E. (CMS/CCIIO); Schankweiler, Thomas W. (CMS/OIS); Oh, Mark U. (CMS/OIS); SHEPHERD, David  
**Subject:** RE: extract mtg Th 4-5?

Gina – I am available to attend a meeting at this time. Dave Shepherd is our security SME. Dave is available on Thursday also, but only by call-in.

We would definitely appreciate any details from a requirements perspective that Tom is able to provide prior to the meeting,

Alan

**From:** Miller, Daniel J. (CMS/OIS) [mailto:daniel.miller2@cms.hhs.gov]  
**Sent:** Tuesday, October 16, 2012 11:20 AM

**To:** Zdanowicz, Gina M. (CMS/CCIIO); NABORS, Alan; O'KEIFF, Jim; OWEN, Whitney

**Cc:** Parish, Elizabeth E. (CMS/CCIIO); Muoneke, Evonne N. (CMS/CCIIO); Davis, Natalie E. (CMS/CCIIO); Schankweiler, Thomas W. (CMS/OIS); Oh, Mark U. (CMS/OIS)

**Subject:** RE: extract mtg Th 4-5?

Thanks Gina: Yes, I discussed with Tom S. this morning and we would use the meeting for Tom to lead us and LMI in mapping out an action path to obtain the ATO, give LMI the information they need to consume in terms of security requirements, and map out the parallel strategy of the steps to take to (in time) enable the analytics to be performed in the Cloud. The meeting will be successful if we walk out of the call with milestones and timelines to achieve those objectives.

And per your second question Gina, if you all could identify the best security SME on the LMI side for Tom to begin corresponding with directly; Tom can cc us on e-mails, but will start pulling together different security documents (even before Thursday) and it will help if LMI can make available their security lead to begin trading information back and forth more rapidly than waiting for a collecting meeting/call.

Finally, I'll be here in Bethesda Thursday physically but Tom will likely dial in from Baltimore.

Thanks guys!

**Daniel J. Miller**

Deputy Director, Division of Application and Data Services (DADS)

Consumer Information & Insurance Systems Group (CIISG)

Office of Information Services (OIS) - Centers for Medicare & Medicaid Services (CMS)

U.S. Department of Health & Human Services (DHHS)

Mobile Phone (bb): (b)(6) | Office Phone: (301) 492-4364

[daniel.miller2@cms.hhs.gov](mailto:daniel.miller2@cms.hhs.gov) | [www.healthcare.gov](http://www.healthcare.gov)

**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:** Zdanowicz, Gina M. (CMS/CCIIO)

**Sent:** Tuesday, October 16, 2012 10:23 AM

**To:** NABORS, Alan; O'KEIFF, Jim; OWEN, Whitney

**Cc:** Parish, Elizabeth E. (CMS/CCIIO); Muoneke, Evonne N. (CMS/CCIIO); Davis, Natalie E. (CMS/CCIIO); Miller, Daniel J. (CMS/OIS)

**Subject:** extract mtg Th 4-5?

Hello – just wondering if you are available to meet this Thursday from 4-5 to talk with Tom S., Mark, and OIS. Also, can you please id your key security POC? Dan – please jump in with additional details. LMI – please let us know if you have any questions.

Thanks,

Gina

Gina Zdanowicz

Office of Health Insurance Exchanges

Center for Consumer Information & Insurance Oversight

Centers for Medicare & Medicaid Services, DHHS

301-492-4451

Information Not Releasable to the Public Unless Authorized by Law: This information has not been publically 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.

Message

**From:** Trenkle, Tony (CMS/OIS); [Redacted] NotResp  
[Redacted] NotResp  
**Sent:** 10/23/2013 11:12:22 PM  
**To:** Schankweiler, Thomas W. (CMS/OIS); [Redacted] NotResp  
[Redacted] NotResp; Fryer, Teresa M. (CMS/OIS); [Redacted] NotResp  
[Redacted] NotResp; Linares, George E. (CMS/OIS)  
[Redacted] NotResp; Outerbridge,  
Monique (CMS/OIS); [Redacted] NotResp  
Grothe, Kirk A. (CMS/OIS); [Redacted] NotResp  
[Redacted] NotResp; Chao, Henry (CMS/OIS); [Redacted] NotResp  
[Redacted] NotResp  
**Subject:** Re: Security Report

Thanks Tom

**From:** Schankweiler, Thomas W. (CMS/OIS)  
**Sent:** Wednesday, October 23, 2013 07:06 PM  
**To:** Trenkle, Tony (CMS/OIS); Fryer, Teresa M. (CMS/OIS); Linares, George E. (CMS/OIS); Outerbridge, Monique (CMS/OIS); Grothe, Kirk A. (CMS/OIS); Chao, Henry (CMS/OIS)  
**Subject:** Re: Security Report

We will have a marketplace analyst contact hhs to review the details of this report and will prepare a remediation plan.

Regards,

Tom

**From:** Trenkle, Tony (CMS/OIS)  
**Sent:** Wednesday, October 23, 2013 06:57 PM  
**To:** Fryer, Teresa M. (CMS/OIS); Linares, George E. (CMS/OIS); Outerbridge, Monique (CMS/OIS); Grothe, Kirk A. (CMS/OIS); Chao, Henry (CMS/OIS); Schankweiler, Thomas W. (CMS/OIS)  
**Subject:** Fw: Security Report

**From:** Baitman, Frank (OS/ASA/OCIO)  
**Sent:** Wednesday, October 23, 2013 06:45 PM  
**To:** Snyder, Michelle (CMS/OA); Trenkle, Tony (CMS/OIS)  
**Cc:** Charest, Kevin (OS/ASA/OCIO/OIS); Fryer, Teresa M. (CMS/OIS)  
**Subject:** FW: Security Report

Michelle and Tony,

In my last communication, I indicated that Brad Ellison was continuing to investigate security issues associated with the Marketplaces: he's done a great job in recent days! While his work continues, I wanted to share with you specific vulnerabilities that have been identified to date.

We're happy to work with your team to address remediation for these and other vulnerabilities — please feel free to work directly with Kevin Charest to tap into our Security team.

- Frank

**From:** Ellison, Brad (ASA/OCIO/OIS/CSIRC)  
**Sent:** Wednesday, October 23, 2013 12:03 PM  
**To:** Charest, Kevin (OS/ASA/OCIO/OIS)  
**Cc:** Graham, Jeffery (ASA/OCIO/OIS/CSIRC)  
**Subject:** RE: Report

The system in question may be using faulty NotResp in a production environment. (Details withheld)

NotResp

**NotResp**

**From:** Charest, Kevin (OS/ASA/OCIO/OIS)  
**Sent:** Monday, October 21, 2013 1:10 PM  
**To:** Ellison, Brad (ASA/OCIO/OIS/CSIRC)  
**Cc:** Graham, Jeffery (ASA/OCIO/OIS/CSIRC)  
**Subject:** RE: Report

Brad where are the comments on the logs available and not available? How about the suggestion that the **Not** **Res** should be merged with the **NotResp** ?

**From:** Ellison, Brad (ASA/OCIO/OIS/CSIRC)  
**Sent:** Monday, October 21, 2013 12:53 PM  
**To:** Charest, Kevin (OS/ASA/OCIO/OIS)  
**Cc:** Graham, Jeffery (ASA/OCIO/OIS/CSIRC)  
**Subject:** RE: Report

Kevin,

NotResp



NotResp

Thanks,

Brad Ellison, CISSP

CSIRC Manager, Cybersecurity Operations

US Department of Health and Human Services

(404) 235-2824 - Office

(b)(6)

Cell

[Brad.Ellison@hhs.gov](mailto:Brad.Ellison@hhs.gov)

**From:** Charest, Kevin (OS/ASA/OCIO/OIS)  
**Sent:** Monday, October 21, 2013 12:20 PM  
**To:** Ellison, Brad (ASA/OCIO/OIS/CSIRC)  
**Subject:** Report

Brad,

When can I expect the report on CMS? I had asked for it by noon.

Kevin

Kevin Charest Ph.D., CISSP, PMP

Chief Information Security Officer

U.S. Department of Health and Human Services

Email: [Kevin.Charest@hhs.gov](mailto:Kevin.Charest@hhs.gov)

(b)(6)

Ofc. 202-690-5548; Mobile: (b)(6)

*"Driving secure solutions through innovation and sustainable business practices"*

Message

**From:** Trenkle, Tony (CMS/OIS) NotResp  
NotResp  
**Sent:** 10/23/2013 11:39:55 PM  
**To:** Snyder, Michelle (CMS/OA) NotResp  
Baitman, Frank (OS/ASA/OCIO) NotResp  
NotResp  
**CC:** Charest, Kevin (OS/ASA/OCIO/OIS) NotResp Fryer,  
Teresa M. (CMS/OIS) NotResp  
NotResp Schankweiler, Thomas W. (CMS/OIS) NotResp  
NotResp Outerbridge, Monique (CMS/OIS)  
NotResp  
**Subject:** Re: Security Report

Frank

Tom is looking into Brad's information and will be getting back to us.

**From:** Snyder, Michelle (CMS/OA)  
**Sent:** Wednesday, October 23, 2013 07:28 PM  
**To:** Baitman, Frank (OS/ASA/OCIO); Trenkle, Tony (CMS/OIS)  
**Cc:** Charest, Kevin (OS/ASA/OCIO/OIS); Fryer, Teresa M. (CMS/OIS)  
**Subject:** Re: Security Report

Thanks Frank. Good timing for a discussion

Michelle

-----  
Sent from my BlackBerry Wireless Device

**From:** Baitman, Frank (OS/ASA/OCIO)  
**Sent:** Wednesday, October 23, 2013 06:45 PM  
**To:** Snyder, Michelle (CMS/OA); Trenkle, Tony (CMS/OIS)  
**Cc:** Charest, Kevin (OS/ASA/OCIO/OIS); Fryer, Teresa M. (CMS/OIS)  
**Subject:** FW: Security Report

Michelle and Tony,

In my last communication, I indicated that Brad Ellison was continuing to investigate security issues associated with the Marketplaces: he's done a great job in recent days! While his work continues, I wanted to share with you specific vulnerabilities that have been identified to date.

We're happy to work with your team to address remediation for these and other vulnerabilities — please feel free to work directly with Kevin Charest to tap into our Security team.

- Frank

**From:** Ellison, Brad (ASA/OCIO/OIS/CSIRC)  
**Sent:** Wednesday, October 23, 2013 12:03 PM  
**To:** Charest, Kevin (OS/ASA/OCIO/OIS)  
**Cc:** Graham, Jeffery (ASA/OCIO/OIS/CSIRC)  
**Subject:** RE: Report

The system in question may be using NotResp in a production environment. (Details withheld)

NotResp

NotResp

**From:** Charest, Kevin (OS/ASA/OCIO/OIS)  
**Sent:** Monday, October 21, 2013 1:10 PM  
**To:** Ellison, Brad (ASA/OCIO/OIS/CSIRC)  
**Cc:** Graham, Jeffery (ASA/OCIO/OIS/CSIRC)  
**Subject:** RE: Report

Brad where are the comments on the logs available and not available? How about the suggestion that the **NotResp** could be merged with the **NotResp**

**From:** Ellison, Brad (ASA/OCIO/OIS/CSIRC)  
**Sent:** Monday, October 21, 2013 12:53 PM  
**To:** Charest, Kevin (OS/ASA/OCIO/OIS)  
**Cc:** Graham, Jeffery (ASA/OCIO/OIS/CSIRC)  
**Subject:** RE: Report

Kevin,

**NotResp**

NotResp

Thanks,



Brad Ellison, CISSP

CSIRC Manager, Cybersecurity Operations

US Department of Health and Human Services

(404) 235-2824 - Office

(b)(6)

Cell

[Brad.Ellison@hhs.gov](mailto:Brad.Ellison@hhs.gov)

**From:** Charest, Kevin (OS/ASA/OCIO/OIS)  
**Sent:** Monday, October 21, 2013 12:20 PM  
**To:** Ellison, Brad (ASA/OCIO/OIS/CSIRC)  
**Subject:** Report

Brad,

When can I expect the report on CMS? I had asked for it by noon.

Kevin

Kevin Charest Ph.D., CISSP, PMP

Chief Information Security Officer

U.S. Department of Health and Human Services

Email: [Kevin.Charest@hhs.gov](mailto:Kevin.Charest@hhs.gov)

(b)(6)

Ofc. 202-690-5548; Mobile (b)(6)

*"Driving secure solutions through innovation and sustainable business practices"*

Message

**From:** Trenkle, Tony (CMS/OIS) [NotResp]  
[NotResp]  
**Sent:** 10/26/2013 1:07:44 PM  
**To:** Schankweiler, Thomas W. (CMS/OIS) [NotResp]  
[NotResp] Fryer, Teresa M. (CMS/OIS) [NotResp]  
[NotResp] [NotResp] Linares, George E. (CMS/OIS)  
[NotResp] Outerbridge,  
Monique (CMS/OIS) [NotResp]  
Grothe, Kirk A. (CMS/OIS) [NotResp]  
[NotResp] Chao, Henry (CMS/OIS) [NotResp]  
[NotResp]  
**CC:** Lyles, Darrin V. (CMS/OIS) [NotResp]  
[NotResp]  
**Subject:** Re: Security Report - Feedback

Thanks Tom. This is very helpful. Please keep us informed on any department activities because Frank will be looking for responses to any issues reported to him. BTW we did talk to [NotResp] yesterday regarding concerns over [NotResp] handling of the logs and the transition work. I believe that they will be better at responding from here on.

Thanks again for all of your work and for taking the time to talk to Patty yesterday evening.

**From:** Schankweiler, Thomas W. (CMS/OIS)  
**Sent:** Saturday, October 26, 2013 08:58 AM  
**To:** Trenkle, Tony (CMS/OIS); Fryer, Teresa M. (CMS/OIS); Linares, George E. (CMS/OIS); Outerbridge, Monique (CMS/OIS); Grothe, Kirk A. (CMS/OIS); Chao, Henry (CMS/OIS)  
**Cc:** Lyles, Darrin V. (CMS/OIS)  
**Subject:** Re: Security Report - Feedback

Tony,

Sorry for the delay in responding to this inquiry. The [NotResp] re-branded from [NotResp] Team] reviewed the information provided by Brad and they direct made contact with the HHS CSIRT to inquire further. The information Brad provided is information that the [NotResp] analysts provided to [NotResp] during his site visit. HHS was simply reviewing and confirming the threats and making a report to Frank and Kevin that these are weaknesses being worked. [NotResp] has confirmed that HHS CIRT has not yet started testing or independently investigating of their own. Finally, the weaknesses listed are documented and are being worked by various contractors.

Each time an application weakness is identified the [NotResp] opens up a Category-7 ticket in [NotResp] or "application vulnerability" and notifies the appropriate contractor. CAT-7 are not considered security events nor incidents as there is not an attempt to exploit nor an active exploitation occurring. Tickets are then tracked to completion. [NotResp] staff are being provided access and training on [NotResp] and we will soon be switching from [NotResp] as our primary reporting and tracking method.

In regards to log reporting request, Friday was a good day as HHS confirmed that they now have access to the [NotResp] and the logs and they can now perform oversight responsibilities like they do in at the [NotResp] [NotResp] will also be alerted at the same time HHS CSIRT is alerted on a match against any rules/signatures that they create. Folks

are still working through the list of items that was identified by HHS during their site visit, but we are also looking for HHS to complete two support activities. 1) We are seeking US-Cert E-mail accounts, which requires sponsorship by Brad, and second is to work with [NotRes] to have our security clearances checked and held by [NotResp]. Brad mentioned that he has some intelligence information he wants to share with us so we are eager to get this moving. I am planning to follow up with Kevin this weekend to see what information is needed to get item #2.

If you have any questions, please let me know.

Regards,

Tom

**From:** Schankweiler, Thomas W. (CMS/OIS)  
**Sent:** Wednesday, October 23, 2013 7:06 PM  
**To:** Trenkle, Tony (CMS/OIS); Fryer, Teresa M. (CMS/OIS); Linares, George E. (CMS/OIS); Outerbridge, Monique (CMS/OIS); Grothe, Kirk A. (CMS/OIS); Chao, Henry (CMS/OIS)  
**Subject:** Re: Security Report

We will have a marketplace analyst contact hhs to review the details of this report and will prepare a remediation plan.

Regards,

Tom

**From:** Trenkle, Tony (CMS/OIS)  
**Sent:** Wednesday, October 23, 2013 06:57 PM  
**To:** Fryer, Teresa M. (CMS/OIS); Linares, George E. (CMS/OIS); Outerbridge, Monique (CMS/OIS); Grothe, Kirk A. (CMS/OIS); Chao, Henry (CMS/OIS); Schankweiler, Thomas W. (CMS/OIS)  
**Subject:** Fw: Security Report

**From:** Baitman, Frank (OS/ASA/OCIO)  
**Sent:** Wednesday, October 23, 2013 06:45 PM  
**To:** Snyder, Michelle (CMS/OA); Trenkle, Tony (CMS/OIS)  
**Cc:** Charest, Kevin (OS/ASA/OCIO/OIS); Fryer, Teresa M. (CMS/OIS)  
**Subject:** FW: Security Report

Michelle and Tony,

In my last communication, I indicated that Brad Ellison was continuing to investigate security issues associated with the Marketplaces: he's done a great job in recent days! While his work continues, I wanted to share with you specific vulnerabilities that have been identified to date.

We're happy to work with your team to address remediation for these and other vulnerabilities — please feel free to work directly with Kevin Charest to tap into our Security team.

- Frank

**From:** Ellison, Brad (ASA/OCIO/OIS/CSIRC)  
**Sent:** Wednesday, October 23, 2013 12:03 PM  
**To:** Charest, Kevin (OS/ASA/OCIO/OIS)  
**Cc:** Graham, Jeffery (ASA/OCIO/OIS/CSIRC)  
**Subject:** RE: Report

The system in question may be using faulty  
environment. (Details withheld)

NotResp

in a production

NotResp

NotResp

**From:** Charest, Kevin (OS/ASA/OCIO/OIS)  
**Sent:** Monday, October 21, 2013 1:10 PM  
**To:** Ellison, Brad (ASA/OCIO/OIS/CSIRC)

**Cc:** Graham, Jeffery (ASA/OCIO/OIS/CSIRC)

**Subject:** RE: Report

Brad where are the comments on the logs available and not available? How about the suggestion that the NotR  
esp should be merged with the NotResp

**From:** Ellison, Brad (ASA/OCIO/OIS/CSIRC)

**Sent:** Monday, October 21, 2013 12:53 PM

**To:** Charest, Kevin (OS/ASA/OCIO/OIS)

**Cc:** Graham, Jeffery (ASA/OCIO/OIS/CSIRC)

**Subject:** RE: Report

Kevin,

NotResp

NotResp

Thanks,

Brad Ellison, CISSP

CSIRC Manager, Cybersecurity Operations



US Department of Health and Human Services

(404) 235-2824 - Office

(b)(6)

- Cell

Brad.Ellison@hhs.gov

**From:** Charest, Kevin (OS/ASA/OCIO/OIS)

**Sent:** Monday, October 21, 2013 12:20 PM

**To:** Ellison, Brad (ASA/OCIO/OIS/CSIRC)

**Subject:** Report

Brad,

When can I expect the report on CMS? I had asked for it by noon.

Kevin

Kevin Charest Ph.D., CISSP, PMP

Chief Information Security Officer

U.S. Department of Health and Human Services

Email: [Kevin.Charest@hhs.gov](mailto:Kevin.Charest@hhs.gov)

NotResp

Ofc. 202-690-5548; Mobile (b)(6)

CMS000866

*"Driving secure solutions through innovation and sustainable business practices"*

Message

**From:** Chao, Henry (CMS/OIS) [NotResp]  
**Sent:** 9/22/2013 5:36:38 PM  
**To:** Schankweiler, Thomas W. (CMS/OIS) [NotResp]  
 [NotResp] Lyles, Darrin V. (CMS/OIS) [NotResp]  
**CC:** [NotResp]  
 Outerbridge, Monique (CMS/OIS) [NotResp]  
 [NotResp] Grothe, Kirk A. (CMS/OIS) [NotResp]  
 [NotResp]  
**Subject:** Re: SCA Finding Analysis

So using the BDC or an EDC to illustrate an analogous situation of which I am certain there are historical precedences even just in the tenure of Teresa, combining what the XOSC found with the final SCA would be similar to saying that current high open findings anywhere in a data center would translated as a lack of confidence in any one system that is in that data center. To take it a step further that means we should apply the 17 findings to CALT, MIDAS, Hub, zONE, HIOS, EIDM, and Healthcare.gov.

Or am I mixing things up?

I want you to go find me similar situation where we would apply the 17 findings from a global test to a single ATO for a single system. For example CMSNet high findings, BDC high findings, any of the VDCs or any other data center High Findings that then is applied to each systems ATO evaluation.

Henry Chao  
 Deputy Chief Information Officer and Deputy Director  
 Office of Information Services  
 Centers for Medicare & Medicaid Services  
 7500 Security Blvd  
 Baltimore, MD 21244  
 301-492-4100 (Pri)  
 410-786-1800 (Alt)  
 (b)(6) (BB)

**From:** Schankweiler, Thomas W. (CMS/OIS)  
**Sent:** Sunday, September 22, 2013 01:16 PM  
**To:** Chao, Henry (CMS/OIS); Lyles, Darrin V. (CMS/OIS)  
**Cc:** Outerbridge, Monique (CMS/OIS); Grothe, Kirk A. (CMS/OIS)  
**Subject:** RE: SCA Finding Analysis

Henry,

Cheryl's response shows the feedback to the MITRE/Blue Canopy test that occurred during the week.

What Monica has been given is the list of findings that have been compiled and provided each night over the past five weeks to the test team. The findings come from the testing by the XOC security team. They are all contained in the Sat 12:56 PM file that I sent over to you. These findings are not part of the SCA report, but Teresa is factoring these in as independent testing upon which she is making her decision to recommend that an ATO not be authorized. I had no idea

until Friday that she was going to take this stance. I talked with Monica and Eric on Thursday before I left Herndon and Eric was going to have an updated stats on all the high items. To help expedite things, I am planning to have Adam Willard report on Monday to Herndon to work with Eric to confirm the status of each of these.

Does that help clarify? If not I can call you.

Tom

**From:** Chao, Henry (CMS/OIS)  
**Sent:** Saturday, September 21, 2013 6:25 PM  
**To:** Schankweiler, Thomas W. (CMS/OIS); Lyles, Darrin V. (CMS/OIS)  
**Cc:** Outerbridge, Monique (CMS/OIS); Grothe, Kirk A. (CMS/OIS)  
**Subject:** Re: SCA Finding Analysis

Tom,

To answer your earlier email Cheryl's response is based on you asking me to follow up with Monica on the 17 high findings the XOSC has on the books and you made it sound like they will be part of the report.

So give me the full story. What are we actually signing off on and what finding are indicated by whom. Seems confusing that the recent FFM SCA and accompanying report can have input from other security testing sources?

Bottom line is on Monday Marilyn and Michelle want the clean and simple explanation--what is the risk we are assuming--facts, not what someone feels.

Henry Chao  
Deputy Chief Information Officer and Deputy Director  
Office of Information Services  
Centers for Medicare & Medicaid Services  
7500 Security Blvd  
Baltimore, MD 21244  
301-492-4100 (Pri)  
410-786-1800 (Alt)  
(b)(6) (BB)

**From:** Schankweiler, Thomas W. (CMS/OIS)  
**Sent:** Saturday, September 21, 2013 05:59 PM  
**To:** Chao, Henry (CMS/OIS); Lyles, Darrin V. (CMS/OIS)  
**Cc:** Outerbridge, Monique (CMS/OIS); Grothe, Kirk A. (CMS/OIS)  
**Subject:** RE: SCA Finding Analysis

Henry,

This matches what I would expect from the SCA audit. However, this is not the response to the High items though. I have arranged for Adam Willard of FGS to come to Herndon on Monday and Tuesday to work with Eric (CGI) about reviewing and closing out the items from his list. I have to be in Baltimore for some security meeting with Tony and George. When I get done there I'll head to Herndon for the evening.

Darrin is working with the SCA team on Monday for the Adobe Live Cycle (Digi-Docs) review.

I have a request in to Teresa to have Kevin and a guy named Jason Patterson to come up to Baltimore on Tue/Wed to sit with someone on her POAM team to work through and close out as many findings as possible. Part of the challenge is getting everything documented just-so in the CFACTS system so it will be acceptably closed. Hopefully a side by session will result in a 35-40% reduction in overall findings which are actually resolved, but still need to pass the CFACTS POAM audit process.

Finally, Kirk and I had a discussion with Teresa on Friday, and after Oct 1, we are going to sit down collectively with OAGM to find out how to mod the Blue Canopy contract so that we can get a dedicated test team for the next year to work in line on FFM and DSH testing. The constraints of having to test within a rigid timeframe and with limited scopes has been a barrier for getting testers to support the ad-hoc nature of the build process we have been and will continue to operate in. Folks have worked hard to be flexible but to stay within the contract boundaries. The best thing we can do is address the restrictions around the barrier so that we have the freedom to perform more ad-hoc testing on demand.

In regards to tools, we will continue to work with Peter, and Mark Orlando and I will be there to talk about the tools. I am not sure we have much in the way of overlap, like Splunk and Akamai, the tool and service can support both operations and security. Splunk has logs being fed to it which are not duplicative of other logs being captured elsewhere. Hope to explain more of that approach later this week.

Thanks,

Tom

**From:** Chao, Henry (CMS/OIS)

**Sent:** Saturday, September 21, 2013 5:02 PM

**To:** Campbell, Cheryl (CGI Federal); Schankweiler, Thomas W. (CMS/OIS); Lyles, Darrin V. (CMS/OIS)

**Cc:** Ramamoorthy, Balaji Manikandan (CGI Federal); Martin, Rich (CGI Federal); Outerbridge, Monique (CMS/OIS)

**Subject:** RE: SCA Finding Analysis

**Importance:** High

Tom,

Does this match what you were expecting?

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

Centers for Medicare & Medicaid Services  
410-786-1800

**From:** Campbell, Cheryl (CGI Federal) [<mailto:Cheryl.Campbell@cgifederal.com>]  
**Sent:** Saturday, September 21, 2013 4:51 PM  
**To:** Chao, Henry (CMS/OIS)  
**Cc:** Ramamoorthy, Balaji Manikandan (CGI Federal); Martin, Rich (CGI Federal)  
**Subject:** FW: SCA Finding Analysis

Henry,

As per our discussion earlier today, Balaji has provided an update on the 2 High and 17 Moderate findings identified and CGI's mitigation/action.

As part of the latest round of Mitre and Blue Canopy SCA Testing that was completed on Friday, September 20th, there were a total of 2 High and 17 Moderate findings identified. These finding can be grouped into 5 different categories:

Category	High	Moderate
Access Control	1	5
Session Management	1	
Documentation		3
Contingency & Planning		1
System and Communication Protection		6
System and Information Integrity		2
<b>Total Findings</b>	<b>2</b>	<b>17</b>

An initial analysis is attached with tentative target dates. As part of our initial review and planning, four of the findings have already been closed (2 high / 3 moderate) and two others are pending a review by Mitre. Of the remaining, there are seven moderate findings that are still outstanding and we have developed a tentative plan as to when these findings will be addressed. However, there are five moderate findings that cannot be closed due to limitations based upon CMS requirements or the way in which the system has been architected. These findings will need to be reviewed with CMS to determine the risk threshold and next steps. The table below summarizes the status of 2 High and 17 Moderate Findings

Status	High	Moderate
Closed	2	3
Outstanding		7
Pending		2
Limitation		5
<b>Total Findings</b>	<b>2</b>	<b>17</b>

Attached is the SCA Testing Report Summary with detailed information on each finding.

Balaji is here today in Herndon and is prepared to discuss at your convenience.

Let him know if you want to meet today.

Cheryl

Message

**From:** Trenkle, Tony [NotResp]  
[NotResp]  
**Sent:** 11/8/2013 12:14:14 AM  
**To:** Boulanger, Jennifer L. (CMS) [NotResp]  
[NotResp]  
[NotResp] Schankweiler, Thomas W.  
[NotResp]  
**CC:** Nelson, David J. (CMS/OEM) [NotResp]  
[NotResp] Chao, Henry (CMS/OIS) [NotResp]  
[NotResp] Aronson, Lauren (CMS/OL) [NotResp]  
[NotResp] Bradley, Tasha (CMS/OC)  
[NotResp]  
**Subject:** Re: Compilation of statements/ background on security

Rob Tagalicod and Maribel Franey

**From:** Boulanger, Jennifer L. (CMS)  
**Sent:** Thursday, November 07, 2013 07:08 PM  
**To:** Trenkle, Tony (CMS/OIS); Fryer, Teresa M. (CMS/OIS); Schankweiler, Thomas W. (CMS/OIS)  
**Cc:** Nelson, David J. (CMS/OEM); Chao, Henry (CMS/OIS); Aronson, Lauren (CMS/OL); Bradley, Tasha (CMS/OC)  
**Subject:** RE: Compilation of statements/ background on security

Tony, I did not – thanks for flagging. Who is [NotResp] needs to see?

**From:** Trenkle, Tony (CMS/OIS)  
**Sent:** Thursday, November 07, 2013 6:53 PM  
**To:** Boulanger, Jennifer L. (CMS); Fryer, Teresa M. (CMS/OIS); Schankweiler, Thomas W. (CMS/OIS)  
**Cc:** Nelson, David J. (CMS/OEM); Chao, Henry (CMS/OIS); Aronson, Lauren (CMS/OL); Bradley, Tasha (CMS/OC)  
**Subject:** Re: Compilation of statements/ background on security

Jennifer

Did you run the privacy statements past [NotResp] Mitre is not testing. Teresa and Tom can provide input on Monitoring and penetration testing as well as any other activities Tom's team is doing.

**From:** Boulanger, Jennifer L. (CMS)  
**Sent:** Thursday, November 07, 2013 06:15 PM  
**To:** Trenkle, Tony (CMS/OIS); Fryer, Teresa M. (CMS/OIS); Schankweiler, Thomas W. (CMS/OIS)  
**Cc:** Nelson, David J. (CMS/OEM); Chao, Henry (CMS/OIS); Aronson, Lauren (CMS/OL); Bradley, Tasha (CMS/OC)  
**Subject:** FW: Compilation of statements/ background on security

Tony and Tom,

Below is a compilation of statements that have been made on security that ASPA is working on. Could you please look at these and give me any comments ASAP? I am worried about the statements about mitre. Is there anyone else who should comment? We are being asked to provide comments by 9am and I am sorry for the overly short timeframe. (anything you can give me is appreciated – even if after 9am.)

CMS000873



Thanks so much!

Jennifer

**Draft/ Pre-Decisional/ Not for Distribution**

## **Security: Clearing up the Facts**

**Statement from HHS spokesperson:** “The privacy and security of consumers personal information is a top priority for us. When consumers fill out their online marketplace applications they can trust that the information that they are providing is protected by stringent security standards. Security testing happens on an ongoing basis using industry best practices to appropriately safeguard consumers personal information.”

(b)(5)

(b)(5)

### **From CMS Data Hub Fact Sheet:**

CMS developed the marketplace systems consistent with federal statutes, guidelines and industry standards that ensure the security, privacy, and integrity of systems and the data that flows through them. All of CMS’ marketplace systems of records are subject to the Privacy Act of 1974, the Computer Security Act of 1987, and the Federal Information Security Management Act of 2002. These systems must also comply with various rules and regulations promulgated by HHS, the Office of Management and Budget, the Department of Homeland Security, and the National Institute of Standards and Technology.

### **Excerpts from Secretary Sebelius: Senate Finance Committee Hearing, 11/6/13**

- (b)(5)
- “Well, I share your concerns about individual privacy. And I would say the site was developed with the highest standards in mind. It is FISMA (ph) certified, which is the federal standard. It meets the NIST standards.”
- (b)(5)

### **ADDITIONAL BACKGROUND AS NEEDED:**

#### **FISMA authority: How does this work?**

- The six-month authorization to operate is a determination that the Federally Facilitated Marketplace (FFM) is FISMA compliant.
- All authorities to operate (ATOs) are required to have a termination date under FISMA guidance. There is currently a six-month authority to operate in place for the FFM. Security testing is happening on an ongoing basis using industry best practices and, as required in the ATO, technical experts are undertaking a number of strategies to mitigate risks. The FFM’s six-month authority to operate is fully FISMA compliant.

(b)(5)

(b)(5)

**Privacy: How are you making sure that you are protecting the privacy of applicants when it comes to personal information?**

- Applications are retained by the FFM in case there is an appeal of the eligibility determination. The security/privacy of the FFM meets the Federal standards for the maintenance of personally identifiable information.
- After attesting to having authority to apply on a family or household member's behalf, individuals filing an application online may submit information about those household members that is subject to verification. The Exchange verifies whether the information submitted by the applicant, such as name, address, or social security number, is consistent with information from data sources, and if not, the individual is asked to provide additional information to resolve the inconsistency. The Exchange does not show information about family or household members received from data sources to the application filer during the application process.
- After consultation with OMB, which is statutorily charged with overseeing and assisting agencies in implementing the Privacy Act, HHS & SSA determined that this use of information for verification purposes is authorized by the Privacy Act as a "routine use."
- The Privacy Act authorizes agencies to disclose agency records as a "routine use" when doing so is "compatible with the purpose for which the information was collected." Because eligibility determinations are among the reasons for which the records are collected, the records' use by the Exchange constitutes a routine use. This is consistent with many other previously established routine uses in which information is provided for purposes of eligibility determinations in health maintenance or other government benefit programs, such as Medicaid, Social Security or LIHEAP.

(b)(5)

(b)(5)

(b)(5)

[i] **NIST Guide for Applying the Risk Management Framework to Federal Information Systems (Appendix F, P F-5)**  
**<http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf>**

### **F.3 AUTHORIZATION DECISION DOCUMENT**

The *authorization decision document* transmits the final security authorization decision from the authorizing official to the information system owner or common control provider and other key organizational officials, as appropriate. The authorization decision document contains the following information:

- Authorization decision;
- Terms and conditions for the authorization;
- Authorization termination date; and
- Risk executive (function) input (if provided).

The security *authorization decision* indicates whether the information system is: (i) authorized to operate; or (ii) not authorized to operate. For common controls, the authorization decision means that the controls are approved for *inheritance* by organizational information systems. The *terms and conditions* for the authorization provide a description of any limitations or restrictions placed on the operation of the information system or the implementation of common controls that must be followed by the system owner or common control provider. The *authorization termination date*, established by the authorizing official, indicates when the security authorization expires and reauthorization is required. An authorizing official designated representative prepares the authorization decision document for the authorizing official with authorization recommendations, as appropriate. The authorization decision document is attached to the original authorization package and transmitted to the information system owner or common control provider.<sup>69</sup>

Upon receipt of the authorization decision document and authorization package, the information system owner or common control provider acknowledges and implements the terms and conditions of the authorization and notifies the authorizing official. The information system owner or common control provider retains the original authorization decision document and authorization package.<sup>70</sup> The organization ensures that authorization documents for information systems and for common controls are available to appropriate organizational officials (e.g., information system owners inheriting common controls, the risk executive [function], chief information officers, senior information security officers, information system security officers). The contents of the security authorization documentation, especially information regarding information system vulnerabilities, are: (i) marked and appropriately protected in accordance with federal/organizational policy; and (ii) retained in accordance with the organization's record retention policy. The authorizing official verifies on an ongoing basis, that the terms and conditions established as part of the authorization are being followed by the information system owner or common control provider.

Message

**From:** Fryer, Teresa M. (CMS/OIS); [NotResp]  
[NotResp]  
**Sent:** 11/8/2013 12:54:45 AM  
**To:** Boulanger, Jennifer L. (CMS); [NotResp]  
[NotResp]; Trenkle, Tony (CMS/OIS); [NotResp]  
[NotResp]; Schankweiler, Thomas W. (CMS/OIS); [NotResp]  
[NotResp]; Tagalicod, Robert (CMS/OEM); [NotResp]  
[NotResp]; Franey, Maribel R. (CMS/OEM)  
**CC:** Nelson, David J. (CMS/OEM); [NotResp]  
[NotResp]; Chao, Henry (CMS/OIS); [NotResp]  
[NotResp]; Aronson, Lauren (CMS/OL); [NotResp]  
[NotResp]; Bradley, Tasha (CMS/OC)  
**Subject:** RE: Compilation of statements/ background on security

I believe Maribel Franey is out of the office, try Theo Wills.

---

**From:** Boulanger, Jennifer L. (CMS)  
**Sent:** Thursday, November 07, 2013 7:39 PM  
**To:** Trenkle, Tony (CMS/OIS); Fryer, Teresa M. (CMS/OIS); Schankweiler, Thomas W. (CMS/OIS); Tagalicod, Robert (CMS/OEM); Franey, Maribel R. (CMS/OEM)  
**Cc:** Nelson, David J. (CMS/OEM); Chao, Henry (CMS/OIS); Aronson, Lauren (CMS/OL); Bradley, Tasha (CMS/OC)  
**Subject:** RE: Compilation of statements/ background on security  
Thanks! + Rob and Maribel

Rob and Maribel, I left you off the original note. Would you take a look at the privacy statement below and give me any comments tomorrow morning?

Thanks so much!

Jennifer

**From:** Boulanger, Jennifer L. (CMS)  
**Sent:** Thursday, November 07, 2013 06:15 PM  
**To:** Trenkle, Tony (CMS/OIS); Fryer, Teresa M. (CMS/OIS); Schankweiler, Thomas W. (CMS/OIS)  
**Cc:** Nelson, David J. (CMS/OEM); Chao, Henry (CMS/OIS); Aronson, Lauren (CMS/OL); Bradley, Tasha (CMS/OC)  
**Subject:** FW: Compilation of statements/ background on security

Tony and Tom,

Below is a compilation of statements that have been made on security that ASPA is working on. Could you please look at these and give me any comments ASAP? I am worried about the statements about mitre. Is there anyone else who should comment? We are being asked to provide comments by 9am and I am sorry for the overly short timeframe. (anything you can give me is appreciated – even if after 9am.)

Thanks so much!

Jennifer

Draft/ Pre-Decisional/ Not for Distribution

**Security: Clearing up the Facts**

**Statement from HHS spokesperson:** “The privacy and security of consumers personal information is a top priority for us. When consumers fill out their online marketplace applications they can trust that the information that they are providing is protected by stringent security standards. Security testing happens on an ongoing basis using industry best practices to appropriately safeguard consumers personal information.

(b)(5)

(b)(5)

**From CMS Data Hub Fact Sheet:**

CMS developed the marketplace systems consistent with federal statutes, guidelines and industry standards that ensure the security, privacy, and integrity of systems and the data that flows through them. All of CMS’ marketplace systems of records are subject to the Privacy Act of 1974, the Computer Security Act of 1987, and the Federal Information Security Management Act of 2002. These systems must also comply with various rules and regulations promulgated by HHS, the Office of Management and Budget, the Department of Homeland Security, and the National Institute of Standards and Technology.

**Excerpts from Secretary Sebelius: Senate Finance Committee Hearing, 11/6/13**

- (b)(5)
- “Well, I share your concerns about individual privacy. And I would say the site was developed with the highest standards in mind. It is FISMA (ph) certified, which is the federal standard. It meets the NIST standards.”
- (b)(5)

**ADDITIONAL BACKGROUND AS NEEDED:****FISMA authority: How does this work?**

- The six-month authorization to operate is a determination that the Federally Facilitated Marketplace (FFM) is FISMA compliant.
- All authorities to operate (ATOs) are required to have a termination date under FISMA guidance. There is currently a six-month authority to operate in place for the FFM. Security testing is happening on an ongoing basis using industry best practices and, as required in the ATO, technical experts are undertaking a number of strategies to mitigate risks. The FFM’s six-month authority to operate is fully FISMA compliant.

(b)(5)

(b)(5)

(b)(5)

**Privacy: How are you making sure that you are protecting the privacy of applicants when it comes to personal information?**

- Applications are retained by the FFM in case there is an appeal of the eligibility determination. The security/privacy of the FFM meets the Federal standards for the maintenance of personally identifiable information.
- After attesting to having authority to apply on a family or household member's behalf, individuals filing an application online may submit information about those household members that is subject to verification. The Exchange verifies whether the information submitted by the applicant, such as name, address, or social security number, is consistent with information from data sources, and if not, the individual is asked to provide additional information to resolve the inconsistency. The Exchange does not show information about family or household members received from data sources to the application filer during the application process.
- After consultation with OMB, which is statutorily charged with overseeing and assisting agencies in implementing the Privacy Act, HHS & SSA determined that this use of information for verification purposes is authorized by the Privacy Act as a "routine use."
- The Privacy Act authorizes agencies to disclose agency records as a "routine use" when doing so is "compatible with the purpose for which the information was collected." Because eligibility determinations are among the reasons for which the records are collected, the records' use by the Exchange constitutes a routine use. This is consistent with many other previously established routine uses in which information is provided for purposes of eligibility determinations in health maintenance or other government benefit programs, such as Medicaid, Social Security or LIHEAP.

(b)(5)



(b)(5)

(b)(5)

<sup>[1]</sup> NIST Guide for Applying the Risk Management Framework to Federal Information Systems (Appendix F, P F-5)  
<http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf>

### F.3 AUTHORIZATION DECISION DOCUMENT

The *authorization decision document* transmits the final security authorization decision from the authorizing official to the information system owner or common control provider and other key organizational officials, as appropriate. The authorization decision document contains the following information:

- Authorization decision;
- Terms and conditions for the authorization;
- Authorization termination date; and
- Risk executive (function) input (if provided).

The security *authorization decision* indicates whether the information system is: (i) authorized to operate; or (ii) not authorized to operate. For common controls, the authorization decision means that the controls are approved for

*inheritance* by organizational information systems. The *terms and conditions* for the authorization provide a description of any limitations or restrictions placed on the operation of the information system or the implementation of common controls that must be followed by the system owner or common control provider. The *authorization termination date*, established by the authorizing official, indicates when the security authorization expires and reauthorization is required. An authorizing official designated representative prepares the authorization decision document for the authorizing official with authorization recommendations, as appropriate. The authorization decision document is attached to the original authorization package and transmitted to the information system owner or common control provider.<sup>69</sup>

Upon receipt of the authorization decision document and authorization package, the information system owner or common control provider acknowledges and implements the terms and conditions of the authorization and notifies the authorizing official. The information system owner or common control provider retains the original authorization decision document and authorization package.<sup>70</sup> The organization ensures that authorization documents for information systems and for common controls are available to appropriate organizational officials (e.g., information system owners inheriting common controls, the risk executive [function], chief information officers, senior information security officers, information system security officers). The contents of the security authorization documentation, especially information regarding information system vulnerabilities, are: (i) marked and appropriately protected in accordance with federal/organizational policy; and (ii) retained in accordance with the organization's record retention policy. The authorizing official verifies on an ongoing basis, that the terms and conditions established as part of the authorization are being followed by the information system owner or common control provider.

Message

**From:** Linares, George E. (CMS/OIS) [NotResp]  
[NotResp]

**Sent:** 9/10/2013 2:58:54 PM

**To:** Coutts, Todd (CMS/OIS) [NotResp]  
[NotResp]  
Chao, Henry (CMS/OIS) [NotResp]  
Thurston, Robert (CMS/CTR) [NotResp]  
Oh, Mark U. (CMS/OIS) [NotResp]  
Outerbridge, Monique (CMS/OIS) [NotResp]  
Margush, Doug C. (CMS/OIS) [NotResp]  
Thomas W. (CMS/OIS) [NotResp]  
Berkley, Katrina (CMS/OIS) [NotResp]  
Rhodes, Rhonda D. (CMS/OIS) [NotResp]  
Um, Peter (CMS/CTR) [NotResp]  
Walter, Stephen J. (CMS/OIS) [NotResp]  
Basavaraju, Venkat (CMS/OIS) [NotResp]  
Zaman, Akhtar (CMS/OIS) [NotResp]  
Donohoe, Paul X. (CMS/OIS) [NotResp]  
Grothe, Kirk A. [NotResp]  
Burke, Sheila M. (CMS/OIS) [NotResp]  
Dill, Walter (CMS/OIS) [NotResp]  
Radcliffe, Glenn D. (CMS/OIS) [NotResp]  
Schmidt, Donna W. (CMS/OIS) [NotResp]  
Feuerberg, Lisa A. (CMS/OIS) [NotResp]  
Lakshmi Manambedu (Lakshmi.Manambedu@cgifederal.com) [NotResp] Martin, Rich (CGI Federal) [Rich.Martin@cgifederal.com]; Sharma, Hemant (CGI Federal) (Hemant.Sharma@cgifederal.com) [Hemant.Sharma@cgifederal.com]; Karlton Kim (kkim@qssinc.com) [kkim@qssinc.com]; Outerbridge, Monique (CMS/OIS) [NotResp] Dunick, Walter T. [NotResp]  
Alvarez, Carlos (CMS/OIS) [NotResp]  
Chao, Bing (CMS/OIS) [NotResp]  
Margush, Doug C. (CMS/OIS) [NotResp]

**CC:** Booth, Jon G. (CMS/OC) [NotResp]  
Wallace, Mary H. (CMS/OC) [NotResp]  
Reilly, Megan C. (CMS/OC) [NotResp]  
Patel, Ketan (CMS/OC) [NotResp]

**Subject:** RE: Day One Pre-flight checklist

**Attachments:** ATT48407; ATT47278

Let's add the following

**Performance & Stress Testing area** – Capture baseline SLAs for system's response time for all components - FFM, HUB, EIDM and Healthcare.gov and establish an aggregate SLA for the overall consumer experience SLA.

**Operations –**

- Operations should document SLAs and monitor system's performance against the documented SLAs
- Consolidated Logs for a holistic view of all systems
- VDC DR Site Status
- Help Desk, Need to document all known nuances and workarounds from the Browser Compatibility testing

***George Linares***

*Acting Chief Technology Officer*

Centers for Medicare & Medicaid Services (CMS)

410.786.2866 [george.linares@cms.hhs.gov](mailto:george.linares@cms.hhs.gov)

7500 Security Blvd., N3-15-25

Baltimore, MD 21244-1850

Need more information? Visit [the OIS website](#).

---

**From:** Coutts, Todd (CMS/OIS)

**Sent:** Monday, September 09, 2013 10:08 AM

**To:** Chao, Henry (CMS/OIS); Linares, George E. (CMS/OIS); Thurston, Robert (CMS/CTR); Oh, Mark U. (CMS/OIS); Outerbridge, Monique (CMS/OIS); Margush, Doug C. (CMS/OIS); Schankweiler, Thomas W. (CMS/OIS); Berkley, Katrina (CMS/OIS); Rhones, Rhonda D. (CMS/OIS); Um, Peter (CMS/CTR); Walter, Stephen J. (CMS/OIS); Basavaraju, Venkat (CMS/OIS); Zaman, Akhtar (CMS/OIS); Donohoe, Paul X. (CMS/OIS); Grothe, Kirk A. (CMS/OIS); Burke, Sheila M. (CMS/OIS); Dill, Walter (CMS/OIS); Radcliffe, Glenn D. (CMS/OIS); Schmidt, Donna W. (CMS/OIS); Feuerberg, Lisa A. (CMS/OIS); Lakshmi Manambedu (Lakshmi.Manambedu@cgifederal.com); Martin, Rich (CGI Federal); Sharma, Hemant (CGI Federal) (Hemant.Sharma@cgifederal.com); Karlton Kim (kkim@qssinc.com); Outerbridge, Monique (CMS/OIS); Dunick, Walter T. (CMS/OIS); Alvarez, Carlos (CMS/OIS); Chao, Bing (CMS/OIS); Margush, Doug C. (CMS/OIS)

**Cc:** Booth, Jon G. (CMS/OC); Wallace, Mary H. (CMS/OC); Reilly, Megan C. (CMS/OC); Patel, Ketan (CMS/OC)

**Subject:** RE: Day One Pre-flight checklist

All,

Here is a draft of a checklist. Please review and add/edit content. I will get something out soon about how/when we will walk through this to make sure we are ready.

<< File: checklist.docx >>

**Todd Coutts**

Centers for Medicare & Medicaid Services

Office of Information Services

301-492-5139 (office) | (b)(6) (mobile) | [todd.coutts1@cms.hhs.gov](mailto:todd.coutts1@cms.hhs.gov)

7700 Wisconsin Ave Bethesda MD 20814 | Location: 9308

---

**From:** Chao, Henry (CMS/OIS)

**Sent:** Thursday, September 05, 2013 8:36 PM

**To:** Coutts, Todd (CMS/OIS); Linares, George E. (CMS/OIS); Thurston, Robert (CMS/CTR); Oh, Mark U. (CMS/OIS); Outerbridge, Monique (CMS/OIS); Margush, Doug C. (CMS/OIS); Schankweiler, Thomas W. (CMS/OIS); Berkley, Katrina (CMS/OIS); Rhones, Rhonda D. (CMS/OIS); Um, Peter (CMS/CTR); Walter, Stephen J. (CMS/OIS); Basavaraju, Venkat (CMS/OIS); Zaman, Akhtar (CMS/OIS); Donohoe, Paul X. (CMS/OIS); Grothe, Kirk A. (CMS/OIS); Burke, Sheila M. (CMS/OIS); Dill, Walter (CMS/OIS); Radcliffe, Glenn D. (CMS/OIS); Schmidt, Donna W. (CMS/OIS); Feuerberg, Lisa A. (CMS/OIS); Lakshmi Manambedu (Lakshmi.Manambedu@cgifederal.com); Martin, Rich (CGI Federal); Sharma, Hemant (CGI Federal) (Hemant.Sharma@cgifederal.com); Karlton Kim (kkim@qssinc.com); Outerbridge, Monique (CMS/OIS); Dunick, Walter T. (CMS/OIS); Alvarez, Carlos (CMS/OIS); Chao, Bing (CMS/OIS); Margush, Doug C. (CMS/OIS)

**Cc:** Booth, Jon G. (CMS/OC); Wallace, Mary H. (CMS/OC); Reilly, Megan C. (CMS/OC); Patel, Ketan (CMS/OC)

**Subject:** RE: Day One Pre-flight checklist

Not sure where we landed on checklists, but we need something and it may be more than one to handle different situations. We also need to adhere to SOPs that are inherently part of the readiness checklist. Checking off items on a pre-flight list does not guarantee a smooth flight. We still have to work as a team to know when hand-offs, check points, collaboration, integration of processes and information, command and control, etc. in order to EFFECTIVELY EXECUTE and respond appropriately to dynamic circumstances.

NotResp

enjoy.

Henry Chao  
Deputy CIO & Deputy Director,  
Office of Information Services  
Centers for Medicare & Medicaid Services  
410-786-1800  
301-492-4456

---

**From:** Coutts, Todd (CMS/OIS)

**Sent:** Tuesday, September 03, 2013 5:49 PM

**To:** Linares, George E. (CMS/OIS); Chao, Henry (CMS/OIS); Thurston, Robert (CMS/CTR); Oh, Mark U. (CMS/OIS); Outerbridge, Monique (CMS/OIS); Margush, Doug C. (CMS/OIS); Schankweiler, Thomas W. (CMS/OIS); Berkley, Katrina (CMS/OIS); Rhones, Rhonda D. (CMS/OIS); Um, Peter (CMS/CTR); Walter, Stephen J. (CMS/OIS); Basavaraju, Venkat (CMS/OIS); Zaman, Akhtar (CMS/OIS); Donohoe, Paul X. (CMS/OIS); Grothe, Kirk A. (CMS/OIS); Burke, Sheila M. (CMS/OIS); Dill, Walter (CMS/OIS); Radcliffe, Glenn D. (CMS/OIS); Schmidt, Donna W. (CMS/OIS); Feuerberg, Lisa A. (CMS/OIS)

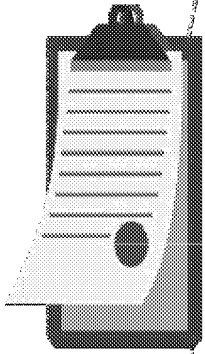
**Cc:** Booth, Jon G. (CMS/OC); Wallace, Mary H. (CMS/OC); Reilly, Megan C. (CMS/OC); Trudel, Karen (CMS/OIS)

**Subject:** RE: Day One Pre-flight checklist

All,

I think we should use portions of the readiness outline we created back in July to drive a checklist. See below. Thoughts?

If this makes sense, George and I can collaborate.



- I. Deployment Overview**
  - Business Goal
  - System Impacted & System Interfaces
  - Architecture Overview
  - High level timeline / milestones
  - Users
  - Volume Forecast
- II. Development & Testing**
  - Development Status
  - Demonstration or walkthrough
  - Deferred functionality
  - Artifact Status
  - Validation Status
    - Functional (internal/external) Testing Results
    - Performance Testing Results
    - Stress Testing Results
  - Development & Testing Readiness Dashboard
- III. Integration Status**
  - Intra-FMPS Integration
  - Integration with other CMS systems (e.g., EIDM)
- IV. Security**
  - SCA Testing Results
  - ATO
  - DR/COOP
  - Security Readiness Dashboard
- V. Infrastructure**
  - Equipment order, install, configuration status
  - Software order, install, configuration status
  - Connectivity configuration status
  - Code Promotion Path & Environmental Readiness
  - Elasticity plans
  - Infrastructure Readiness Dashboard
- VI. Go Live Readiness**
  - User Onboarding (e.g., Trading Partner Agreements, EFT setup)
  - Implementation Plan and Checklists
  - Contact List
  - Escalation Paths
  - Go Live Readiness Dashboard
- VII. Business Operations**
  - Identify supporting business operations
  - Business contractor roles and scope
  - Contractor onboarding and training
  - Business Contractor Readiness
  - Business Operations Readiness Dashboard
- VIII. IT Operations**
  - System error messages and handling
  - Help Desk Readiness
    - Escalation Paths / Help Desk Scripts / Supporting Tools
  - Backup and Recovery
  - Monitoring
  - Job Schedules
  - IT Operations Readiness Dashboard
- IX. External Partners & Users**
  - Agreement Status (e.g., CMA, TPA)
  - Readiness of external partners
    - System readiness
    - Operational readiness
  - Training Plan and Execution
  - External Partners Readiness Dashboard
- X. Risk and Workaround Planning**
  - Non Happy Path Scenarios (e.g., data sources are down, unable to RIDP a consumer)
  - Workaround plan for deferred or downscoped functionality
  - External partners not ready

Focus for Today

Todd Coutts  
Centers for Medicare & Medicaid Services  
Office of Information Services  
301-492-5139 (office) | (b)(6) (mobile) | [todd.coutts1@cms.hhs.gov](mailto:todd.coutts1@cms.hhs.gov)  
7700 Wisconsin Ave Bethesda MD 20814 | Location: 9308

-----Original Message-----

From: Linares, George E. (CMS/OIS)  
Sent: Tuesday, September 03, 2013 10:02 AM  
To: Chao, Henry (CMS/OIS); Thurston, Robert (CMS/CTR); Oh, Mark U. (CMS/OIS); Outerbridge, Monique (CMS/OIS); Margush, Doug C. (CMS/OIS); Schankweiler, Thomas W. (CMS/OIS); Coutts, Todd (CMS/OIS); Berkley, Katrina (CMS/OIS); Rhones, Rhonda D. (CMS/OIS); Um, Peter (CMS/CTR); Walter, Stephen J. (CMS/OIS); Basavaraju, Venkat (CMS/OIS); Zaman, Akhtar (CMS/OIS); Donohoe, Paul X. (CMS/OIS); Grothe, Kirk A. (CMS/OIS); Burke, Sheila M. (CMS/OIS); Dill, Walter (CMS/OIS); Radcliffe, Glenn D. (CMS/OIS); Schmidt, Donna W. (CMS/OIS); Feuerberg, Lisa A. (CMS/OIS)  
Cc: Booth, Jon G. (CMS/OC); Wallace, Mary H. (CMS/OC); Reilly, Megan C. (CMS/OC); Trudel, Karen (CMS/OIS)  
Subject: RE: Day One Pre-flight checklist

I think we should use the attached table in Todd's email as the starting point for the checklist, and we should plan on having an all-day ORR the week of the 23rd, where all the leads can speak to their respective segments. I would add to



the list EIDM as they have things that need to be in place as well.

Thanks

George Linares  
Acting Chief Technology Officer  
Centers for Medicare & Medicaid Services (CMS)  
410.786.2866 george.linares@cms.hhs.gov  
7500 Security Blvd., N3-15-25  
Baltimore, MD 21244-1850

-----Original Message-----

From: Chao, Henry (CMS/OIS)  
Sent: Monday, September 02, 2013 9:29 PM  
To: Thurston, Robert (CMS/CTR); Oh, Mark U. (CMS/OIS); Outerbridge, Monique (CMS/OIS); Margush, Doug C. (CMS/OIS); Schankweiler, Thomas W. (CMS/OIS); Coutts, Todd (CMS/OIS); Berkley, Katrina (CMS/OIS); Rhones, Rhonda D. (CMS/OIS); Um, Peter (CMS/CTR); Walter, Stephen J. (CMS/OIS); Basavaraju, Venkat (CMS/OIS); Zaman, Akhtar (CMS/OIS); Donohoe, Paul X. (CMS/OIS); Grothe, Kirk A. (CMS/OIS); Burke, Sheila M. (CMS/OIS); Dill, Walter (CMS/OIS); Linares, George E. (CMS/OIS); Radcliffe, Glenn D. (CMS/OIS); Schmidt, Donna W. (CMS/OIS)  
Cc: Booth, Jon G. (CMS/OC); Wallace, Mary H. (CMS/OC); Reilly, Megan C. (CMS/OC)  
Subject: Day One Pre-flight checklist

Monique  
Kirk  
Todd  
George,

We're going to need an extensive checklist to go through that not only asks the questions, but also tie actions to how the questions are answered. This is especially true for communicating to Issuers, Caseworkers, Call Centers, Help Desks, States, Agents, Brokers, NAIC, and the federal agencies.

The range of questions need to be wide and deep where necessary. Also this needs to be conducted with different groups and themes (e.g., systems monitoring, Infrastructure and Network, Operations, Security, Production Control including system shut down and disaster recovery, etc.)

So who is working on this?

Katrina--please make sure we have a follow-up on this topic and get a plan finalized.

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  
301-492-4100 (Pri)  
410-786-1800 (Alt)

(b)(6)

(BB)

Message

**From:** Coutts, Todd (CMS/OIS) [NotResp]  
[NotResp]  
**Sent:** 11/25/2013 7:13:01 PM  
**To:** lbjones@mitre.org; Holden, Stacey (CMS/OIS) [NotResp]  
[NotResp]  
**CC:** Schankweiler, Thomas W. (CMS/OIS) [NotResp]  
[NotResp]  
**Subject:** FW: Security Items - Familiar?

Lynn and Stacey,

See below and please get this on the list as high, high priority.

**Todd Coutts**

Centers for Medicare & Medicaid Services  
Office of Information Services  
301-492-5139 (office) | [redacted] (b)(6) (mobile) | [todd.coutts1@cms.hhs.gov](mailto:todd.coutts1@cms.hhs.gov)  
7700 Wisconsin Ave Bethesda MD 20814 | Location: 9308

**From:** Schankweiler, Thomas W. (CMS/OIS)  
**Sent:** Monday, November 25, 2013 1:52 PM  
**To:** Coutts, Todd (CMS/OIS)  
**Subject:** RE: Security Items - Familiar?

Yes, we need these items worked as defects. We can work next to prioritize them, but I was told to get all our security items on the list so that they can be addressed. We are working now to get as many of them as possible cleaned up.

Tom

**From:** Coutts, Todd (CMS/OIS)  
**Sent:** Sunday, November 24, 2013 3:52 PM  
**To:** Schankweiler, Thomas W. (CMS/OIS)  
**Subject:** Security Items - Familiar?  
**Importance:** High

Tom,

A few questions for you:

1. Are you familiar with the Security items in the extract from [redacted] below?
2. If so, do you know if these are already being worked?
3. If not, how would you like to handle them to make sure they get worked? Do you want to work together to get them initiated?

**Todd Coutts**

Centers for Medicare & Medicaid Services  
Office of Information Services  
301-492-5139 (office) | [redacted] (b)(6) (mobile) | [todd.coutts1@cms.hhs.gov](mailto:todd.coutts1@cms.hhs.gov)  
7700 Wisconsin Ave Bethesda MD 20814 | Location: 9308

**From:** Jones, Lynn B. [mailto:lbjones@mitre.org]

**Sent:** Sunday, November 24, 2013 10:59 AM

**To:** Coutts, Todd (CMS/OIS)

**Cc:** Holden, Stacey (CMS/OIS); Cole, Reba R. (CMS/OIS)

**Subject:** IMPORTANT - Decision on NotResp tickets for CCB.

**Importance:** High

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)



(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

Lynn B. Jones  
Principal Multi-Disciplinary Systems Engineer  
The MITRE Corporation

Cell: (b)(6)



Message

**From:** Coutts, Todd (CMS/OIS) [NotResp]  
 [NotResp]  
**Sent:** 12/3/2013 6:46:19 PM  
**To:** Schankweiler, Thomas W. (CMS/OIS) [NotResp]  
 [NotResp]; Garner, John R. (CMS/OA) [NotResp]  
 [NotResp]; Michael Finkel [mfinkel@qssinc.com]  
**CC:** Grothe, Kirk A. (CMS/OIS) [NotResp]  
 [NotResp]; Outerbridge, Monique (CMS/OIS) [NotResp]  
 [NotResp]; Lyles, Darrin V. (CMS/OIS) [NotResp]  
 [NotResp]; Oh, Mark U. (CMS/OIS) [NotResp]  
 [NotResp]; Van, Hung B. (CMS/OIS) [NotResp]  
 [NotResp]; Kane, David (CMS/OIS) [NotResp]  
 [NotResp]; Fender, Rebecca (CMS/CCSQ) [NotResp]  
**Subject:** RE: [NotResp] Checkin

Hi Tom,

We just worked with CGI and it is in testing now. Depending on how the testing looks . . .

- Worst case, it will go into production on 12/9 (Sunday night going into Monday morning)
- Best case, it will go into production on Thursday 12/12 (Wednesday night going into Thursday morning)

**Todd Coutts**

Centers for Medicare & Medicaid Services  
 Office of Information Services

301-492-5139 (office) [b)(6)] mobile) | [todd.coutts1@cms.hhs.gov](mailto:todd.coutts1@cms.hhs.gov)  
 7700 Wisconsin Ave Bethesda MD 20814 | Location: 9308

**From:** Schankweiler, Thomas W. (CMS/OIS)  
**Sent:** Tuesday, December 03, 2013 8:34 AM  
**To:** Coutts, Todd (CMS/OIS); Garner, John R. (CMS/OA); Michael Finkel  
**Cc:** Grothe, Kirk A. (CMS/OIS); Outerbridge, Monique (CMS/OIS); Lyles, Darrin V. (CMS/OIS); Oh, Mark U. (CMS/OIS);  
 Van, Hung B. (CMS/OIS); Kane, David (CMS/OIS)  
**Subject:** RE: [NotResp] Checkin

Todd, Chip, and Mike

Can we get this coordinated for implementation tonight or on Wed at the latest? Which includes coordination with SERCO.

We have security testing beginning on Monday for FFM and SERCO, and it would be ideal if this fix was in place. We also have a number of open items with the department and DHS which are awaiting this fix action to go in place.

Thanks,

Tom

**From:** Fender, Rebecca (CMS/CCSQ)  
**Sent:** Tuesday, November 26, 2013 7:18 PM  
**To:** Schankweiler, Thomas W. (CMS/OIS)  
**Subject:** RE: [REDACTED] NotResp [REDACTED] Checkin

Let me know if you need anything else. I'm not opposed to any direction but I do want it coordinated and I do want to make sure leadership isn't upset and frustrated if SERCO goes down. Honestly if I was picking between the two I would pick to fix the PII. It's a broader issue in my book. Just my humble opinion.

Becky Fender PMP®

CMS

Cell: [REDACTED] (b)(6)

Office 410-786-1006

**From:** Schankweiler, Thomas W. (CMS/OIS)  
**Sent:** Tuesday, November 26, 2013 6:57 PM  
**To:** Fender, Rebecca (CMS/CCSQ); Outerbridge, Monique (CMS/OIS); Basavaraju, Venkat (CMS/OIS)  
**Cc:** Grothe, Kirk A. (CMS/OIS); Oh, Mark U. (CMS/OIS); Van, Hung B. (CMS/OIS); Margush, Doug C. (CMS/OIS); Coutts, Todd (CMS/OIS); Lyles, Darrin V. (CMS/OIS); Fletcher, John A. (CMS/OIS)  
**Subject:** RE: [REDACTED] NotResp [REDACTED] Checkin

Here is my concern. This change will also effect the way consumers pull data. If we launch and we get a drove of people show up on the 30th and their are presented with exposure of PII, we will have a very bad situation on our hands. So now we are faced with the possibility that Serco could be down for days, when it MUST be up, and the possibility of exposing PII and experiencing a new round of political attacks.

I think if we coordinate decisively that we can all make this work. It would mean identifying a roll-back plan, and implementing the changes on Friday morning, testing by SERCO, and rolling-back quickly if it is not successful. I am not sure what all would need to happen to make this happen, but I think we need to launch on the 30th with a reduced risk of PII exposure; that should be the goal.

I'll be on the 9pm call, and hope maybe we can talk about this near the conclusion of the call.

Thanks,

Tom

---

**From:** Fender, Rebecca (CMS/CCSQ)  
**Sent:** Tuesday, November 26, 2013 6:28 PM  
**To:** Schankweiler, Thomas W. (CMS/OIS); Outerbridge, Monique (CMS/OIS); Basavaraju, Venkat (CMS/OIS)  
**Cc:** Grothe, Kirk A. (CMS/OIS); Oh, Mark U. (CMS/OIS); Van, Hung B. (CMS/OIS); Margush, Doug C. (CMS/OIS); Coutts, Todd (CMS/OIS); Lyles, Darrin V. (CMS/OIS); Fletcher, John A. (CMS/OIS)  
**Subject:** RE: [REDACTED] NotResp [REDACTED] Checkin

Hi All,

I just had a quick call with Tom. I am attaching a document I asked CGI to put together a few days ago when this first came to my attention. Again, I agree this needs to take place and is very important but each time we do something with URLs/Servers or Logins we are down for many days with Serco. In fact we were down today due to changes EIDM made. We need to make sure our timing is coordinated(across all contractors), we have appropriate resources available, a rollback plan and possibly do it after hours/early morning. Whatever timing is decided, we need to make sure all

leadership understands the risks to doing it (taking SERCO down) and not doing it (exposing PII). I'm not sure something prior to the 30<sup>th</sup> and our immediate push to clear [NotResp] well with this effort. I will leave it to the group to make recommendations to leadership on timing and priorities.

**Defect numbers are in CALT:** artf161121 / artf161124 and this is part of the List of 65, it is N3 which again was identified to better secure [NotResp] If you have further concerns/questions please reach out to Tom Schankweiler.

**To Test:** Go through normal process as an ESW while someone from our security team is in the backend ensures that [NotResp] (ie. When an ESW closes a completed application) and creates [NotResp] when they search and choose another application to work on or when they click the "Create Application" link.

Let me know if you have questions.

Becky

**Becky Fender PMP®**

CMS

Cel [ (b)(6) ]

Office 410-786-1006

**From:** Schankweiler, Thomas W. (CMS/OIS)

**Sent:** Tuesday, November 26, 2013 5:19 PM

**To:** Outerbridge, Monique (CMS/OIS); Basavaraju, Venkat (CMS/OIS); Fender, Rebecca (CMS/CCSQ)

**Cc:** Grothe, Kirk A. (CMS/OIS); Oh, Mark U. (CMS/OIS); Van, Hung B. (CMS/OIS); Margush, Doug C. (CMS/OIS); Coutts, Todd (CMS/OIS); Lyles, Darrin V. (CMS/OIS); Fletcher, John A. (CMS/OIS)

**Subject:** RE: [NotResp] Checkin

Did this get resolved today? I can participate in a call later tonight.

Tom

**From:** Schankweiler, Thomas W. (CMS/OIS)

**Sent:** Tuesday, November 26, 2013 12:47 PM

**To:** Fender, Rebecca (CMS/CCSQ); Outerbridge, Monique (CMS/OIS); Basavaraju, Venkat (CMS/OIS)

**Cc:** Grothe, Kirk A. (CMS/OIS); Oh, Mark U. (CMS/OIS); Van, Hung B. (CMS/OIS); Margush, Doug C. (CMS/OIS); Coutts, Todd (CMS/OIS); Lyles, Darrin V. (CMS/OIS) ([Darrin.Lyles@cms.hhs.gov](mailto:Darrin.Lyles@cms.hhs.gov)); Fletcher, John A. (CMS/OIS)

**Subject:** RE: [NotResp] Checkin

Rebecca and Monique,

I am inclined to say yes we need this fix put in place. The fix is intended to resolve a serious issue where data, which is not a consumers, is showing up in searches and in xqueries. This is starting to result in a high number of security and privacy incidents, and has a public view to it. We should have a quick meeting about this so CMS can make a final determination. Maybe it could come down, if needed, during this weekend to allow for the test?

Also I am not sure why testing can only be done in prod? Can't another set of self-signed certificates be issued to address this? or is it the case where there is not a matching environment to perform the testing in?

Tom

**From:** Fender, Rebecca (CMS/CCSQ)  
**Sent:** Tuesday, November 26, 2013 10:52 AM  
**To:** Schankweiler, Thomas W. (CMS/OIS); Outerbridge, Monique (CMS/OIS); Basavaraju, Venkat (CMS/OIS)  
**Subject:** FW: [REDACTED] NotResp Checkin  
**Importance:** High

Hi Tom and Monique,

I have serious concerns about this "fix". Every time we do something with the URL we are down for days at SERCO. We can only test this in PROD due to the [REDACTED] NotResp that goes to EIDM and gets passed to ESD. Can you all let me know if you feel we need to take the risk of SERCO being down for a few days? Trust me when I say there is lots of pressure and focus on SERCO and any downtime they incur due to a CGI fix.

Becky

Becky Fender PMP®

CMS

Cell [REDACTED] (b)(6)

Office 410-786-1006

**From:** Fender, Rebecca (CMS/CCSQ)  
**Sent:** Tuesday, November 26, 2013 10:48 AM  
**To:** 'O'Mara, Katyanne J (CGI Federal)'; Minze Chien; Venky Natarajan; Basavaraju, Venkat (CMS/OIS); Niranjan Santhamoorthy; [greg.greshman.health@gmail.com](mailto:greg.greshman.health@gmail.com); Nitin Matta; Girish Shetty; Sundar, Raj N (CGI Federal); Thangavelu, Raja (Non-Member); Ivan Vinogradov; Ramamoorthy, Balaji Manikandan (CGI Federal); Anbu, Bala (Non-Member); Cecilio, Sal (CGI Federal); Roche, Jacqueline R. (CMS/CCIIO)  
**Subject:** RE: [REDACTED] NotResp Checkin

I still do not feel that this is urgent and must happen as a priority. I will discuss with Tom and Monique. I do agree it should happen but I know this will take us down for several days and that simply can't happen at this time. There is NO way to test this other than in prod due to the SAML assertion of their federated login.

Becky Fender PMP®

CMS

Cell [REDACTED] (b)(6)

Office 410-786-1006

**From:** O'Mara, Katyanne J (CGI Federal) [<mailto:katyanne.omara@cgifederal.com>]  
**Sent:** Tuesday, November 26, 2013 10:45 AM  
**To:** Fender, Rebecca (CMS/CCSQ); Minze Chien; Venky Natarajan; Basavaraju, Venkat (CMS/OIS); Niranjan Santhamoorthy; [greg.greshman.health@gmail.com](mailto:greg.greshman.health@gmail.com); Nitin Matta; Girish Shetty; Sundar, Raj N (CGI Federal); Thangavelu, Raja (Non-Member); Ivan Vinogradov; Ramamoorthy, Balaji Manikandan (CGI Federal); Anbu, Bala (Non-Member);

Cecilio, Sal (CGI Federal); Roche, Jacqueline R. (CMS/CCIIO)

**Subject:** RE: [Redacted] heckin

Hi Becky,

I understand your concern.

**Defect numbers are in CALT:** artf161121 / artf161124 and this is part of the List of 65, it is N3 which again was identified to better secure [Redacted] If you have further concerns/questions please reach out to Tom Shankweiler.

**To Test:** Go through normal process as an ESW while someone from our security team is in the backend ensures that [Redacted] i.e. When an ESW closes a completed application) and creates new [Redacted] to work on or when they click the "Create Application" link.

Soumya, Manisha, Eddie and others, even Shaina can be part of the front end testing and Balaji will be assigning someone from his security team to work with us in a coordinated testing effort tomorrow to confirm that the sessions are being created and cleared appropriately.

Our Ops and Security team have completed their tasks. Sal will complete his tasks today. I just need confirmation from EIDM team that they made their change. We will be ready for the coordinated test tomorrow.

I will update the document I sent out with this information.

I hope this answers your questions and alleviates your concerns regarding testing. This is about closing the loop on open sessions, not changing your workflow or affecting your current workflow it's about making your current sessions more secure.

Thanks,

KO

Katy O'Mara | Manager | Health and Compliance Group | CGI Federal

W: 703-227-6411 | C [Redacted] | [www.cgi.com](http://www.cgi.com)

**From:** Fender, Rebecca (CMS/CCSQ) [<mailto:Rebecca.Fender@cms.hhs.gov>]

**Sent:** Tuesday, November 26, 2013 9:58 AM

**To:** O'Mara, Katyanne J (CGI Federal); Minze Chien; Venky Natarajan; Venkat.Basavaraju; Niranjan Santhamoorthy; [greg.greshman.health@gmail.com](mailto:greg.greshman.health@gmail.com); Nitin Matta; Girish Shetty; Sundar, Raj N (CGI Federal); Thangavelu, Raja (Non-Member); Ivan Vinogradov; Ramamoorthy, Balaji Manikandan (CGI Federal); Anbu, Bala (Non-Member); Cecilio, Sal (CGI Federal); Roche, Jacqueline R. (CMS/CCIIO)

**Subject:** RE: [Redacted]

I will try to call in later but have a conflicting meeting with NPC and leadership about the notices issues. Sorry. I really do NOT want to move forward with this until I understand how we plan to test and why this is such a rush as well as how it was discovered. As we know from past experience changes like this can keep SERCO down for days and we cannot afford that at this time.

Becky Fender PMP®

CMS

Cell (b)(6)

Office 410-786-1006

-----Original Appointment-----

**From:** O'Mara, Katyanne J (CGI Federal) [mailto:katyanne.omara@cgifederal.com]

**Sent:** Monday, November 25, 2013 4:20 PM

**To:** O'Mara, Katyanne J (CGI Federal); Minze Chien; Venky Natarajan; Basavaraju, Venkat (CMS/OIS); Niranjana Santhamoorthy; greg.greshman.health@gmail.com; Nitin Matta; Girish Shetty; Sundar, Raj N (CGI Federal); Thangavelu, Raja (Non-Member); Ivan Vinogradov; Ramamoorthy, Balaji Manikandan (CGI Federal); Anbu, Bala (Non-Member); Cecilio, Sal (CGI Federal); Fender, Rebecca (CMS/CCSQ); Roche, Jacqueline R. (CMS/CCIIO)

**Subject:** NotResp Checkin

**When:** Tuesday, November 26, 2013 10:00 AM-10:30 AM (UTC-05:00) Eastern Time (US & Canada).

**Where:** (b)(6)

Hi Everyone,

I'd like to get an update on the tasks below and ensure we are on target for completion for tomorrow afternoon for testing to begin tomorrow night or Wednesday morning in Test 2.

Detailed Technical Action Items:

**EIDM Team Tasks**

1. Currently EIDM is protecting the URL [\(b\)\(6\)](https://(b)(6)) Change the policy to protect the following URL pattern. [\(b\)\(6\)](https://(b)(6))
2. All the header variables remains the same. (NO CHANGES REQUIRED)

NotResp

**FFM Ops Team Tasks**

1. Add the following RP rules for the English

NotResp

2. Restart the Apache RP for the English

#### FFM Security Team Tasks

- 1.
- 2.
- 3.
4. NotResp
- 5.
- 6.
- 7.

#### Application Team Tasks

1. Do a ping to <https://> NotResp every 10 or 15 minutes to keep the EIDM NotResp from the main ESD page. (Please get the guidance from Jeremy)
2. Currently in the NotResp when the ESD worker searches for an NotResp and clicks on the link, it takes the user to the IndividualApp. Instead do a HTTP POST to <https://> NotResp The HTTP POST Parameter should be NotResp



## Message

**From:** Coutts, Todd (CMS/OIS); [Redacted] **NotResp**

**Sent:** 12/3/2013 4:22:44 PM

**To:** Monica Winthrop [monica.winthrop@cgifederal.com]

**CC:** McEachron, Errol (CGI Federal) (Errol.McEachron@cgifederal.com) [Errol.McEachron@cgifederal.com]; 'Venky Natarajan' (vnatarajan@qssinc.com) (vnatarajan@qssinc.com) [vnatarajan@qssinc.com]; Schankweiler, Thomas W. (CMS/OIS); [Redacted] **NotResp**; 'Maglis, Eva' (eva.maglis@cgi.com) [eva.maglis@cgi.com]; Fender, Rebecca (CMS/CCSQ); [Redacted] **NotResp**

**Subject:** FW: [Redacted] **NotResp** Checkin

Monica,

Can you tell me the status of these defects and when they can go in this week? Our security folks are getting heat from the HHS CTO to get these in.

**Defect numbers are in CALT:** artf161121 / artf161124 and this is part of the List of 65, it is N3 which again was identified to better secure [Redacted] **NotResp** If you have further concerns/questions please reach out to Tom Shankweiler

**Todd Coutts**

Centers for Medicare & Medicaid Services  
Office of Information Services

301-492-5139 (office) [Redacted] (b)(6) (mobile) | todd.coutts1@cms.hhs.gov  
7700 Wisconsin Ave Bethesda MD 20814 | Location: 9308

**From:** Schankweiler, Thomas W. (CMS/OIS)

**Sent:** Tuesday, December 03, 2013 8:34 AM

**To:** Coutts, Todd (CMS/OIS); Garner, John R. (CMS/OA); Michael Finkel

**Cc:** Grothe, Kirk A. (CMS/OIS); Outerbridge, Monique (CMS/OIS); Lyles, Darrin V. (CMS/OIS); Oh, Mark U. (CMS/OIS); Van, Hung B. (CMS/OIS); Kane, David (CMS/OIS)

**Subject:** RE: [Redacted] **NotResp** Checkin

Todd, Chip, and Mike

Can we get this coordinated for implementation tonight or on Wed at the latest? Which includes coordination with SERCO.

We have security testing beginning on Monday for FFM and SERCO, and it would be ideal if this fix was in place. We also have a number of open items with the department and DHS which are awaiting this fix action to go in place.

Thanks,

Tom



**From:** Fender, Rebecca (CMS/CCSQ)  
**Sent:** Tuesday, November 26, 2013 7:18 PM  
**To:** Schankweiler, Thomas W. (CMS/OIS)  
**Subject:** RE: [REDACTED] NotResp Checkin

Let me know if you need anything else. I'm not opposed to any direction but I do want it coordinated and I do want to make sure leadership isn't upset and frustrated if SERCO goes down. Honestly if I was picking between the two I would pick to fix the PII. It's a broader issue in my book. Just my humble opinion.

**Becky Fender PMP®**

CMS

Cell: [REDACTED] (b)(6)

Office 410-786-1006

**From:** Schankweiler, Thomas W. (CMS/OIS)  
**Sent:** Tuesday, November 26, 2013 6:57 PM  
**To:** Fender, Rebecca (CMS/CCSQ); Outerbridge, Monique (CMS/OIS); Basavaraju, Venkat (CMS/OIS)  
**Cc:** Grothe, Kirk A. (CMS/OIS); Oh, Mark U. (CMS/OIS); Van, Hung B. (CMS/OIS); Margush, Doug C. (CMS/OIS); Coutts, Todd (CMS/OIS); Lyles, Darrin V. (CMS/OIS); Fletcher, John A. (CMS/OIS)  
**Subject:** RE: [REDACTED] NotResp Checkin

Here is my concern. This change will also effect the way consumers pull data. If we launch and we get a drove of people show up on the 30th and their are presented with exposure of PII, we will have a very bad situation on our hands. So now we are faced with the possibility that Serco could be down for days, when it MUST be up, and the possibility of exposing PII and experiencing a new round of political attacks.

I think if we coordinate decisively that we can all make this work. It would mean identifying a roll-back plan, and implementing the changes on Friday morning, testing by SERCO, and rolling-back quickly if it is not successful. I am not sure what all would need to happen to make this happen, but I think we need to launch on the 30th with a reduced risk of PII exposure; that should be the goal.

I'll be on the 9pm call, and hope maybe we can talk about this near the conclusion of the call.

Thanks,

Tom

---

**From:** Fender, Rebecca (CMS/CCSQ)  
**Sent:** Tuesday, November 26, 2013 6:28 PM  
**To:** Schankweiler, Thomas W. (CMS/OIS); Outerbridge, Monique (CMS/OIS); Basavaraju, Venkat (CMS/OIS)  
**Cc:** Grothe, Kirk A. (CMS/OIS); Oh, Mark U. (CMS/OIS); Van, Hung B. (CMS/OIS); Margush, Doug C. (CMS/OIS); Coutts, Todd (CMS/OIS); Lyles, Darrin V. (CMS/OIS); Fletcher, John A. (CMS/OIS)  
**Subject:** RE: [REDACTED] NotResp  
Hi All,

I just had a quick call with Tom. I am attaching a document I asked CGI to put together a few days ago when this first came to my attention. Again, I agree this needs to take place and is very important but each time we do something with URLs/Servers or Logins we are down for many days with Serco. In fact we were down today due to changes EIDM made. We need to make sure our timing is coordinated(across all contractors), we have appropriate resources available, a rollback plan and possibly do it after hours/early morning. Whatever timing is decided, we need to make sure all leadership understands the risks to doing it (taking SERCO down) and not doing it (exposing PII). I'm not sure something

prior to the 30<sup>th</sup> and our immediate push to clear [NotResp] well with this effort. I will leave it to the group to make recommendations to leadership on timing and priorities.

**Defect numbers are in CALT:** artf161121 / artf161124 and this is part of the List of 65, it is N3 which again was identified to better secure the [NotResp] If you have further concerns/questions please reach out to Tom Schankweiler.

**To Test:** Go through normal process as an ESW while someone from our security team is in the backend ensures that [NotResp] (ie. When an ESW closes a completed application) and creates new [NotResp] when they search and choose another application to work on or when they click the "Create Application" link.

Let me know if you have questions.

Becky

Becky Fender PMP®

CMS

Cell: [NotResp]

Office 410-786-1006

**From:** Schankweiler, Thomas W. (CMS/OIS)

**Sent:** Tuesday, November 26, 2013 5:19 PM

**To:** Outerbridge, Monique (CMS/OIS); Basavaraju, Venkat (CMS/OIS); Fender, Rebecca (CMS/CCSQ)

**Cc:** Grothe, Kirk A. (CMS/OIS); Oh, Mark U. (CMS/OIS); Van, Hung B. (CMS/OIS); Margush, Doug C. (CMS/OIS); Coutts, Todd (CMS/OIS); Lyles, Darrin V. (CMS/OIS); Fletcher, John A. (CMS/OIS)

**Subject:** RE: [NotResp] Checkin

Did this get resolved today? I can participate in a call later tonight.

Tom

**From:** Schankweiler, Thomas W. (CMS/OIS)

**Sent:** Tuesday, November 26, 2013 12:47 PM

**To:** Fender, Rebecca (CMS/CCSQ); Outerbridge, Monique (CMS/OIS); Basavaraju, Venkat (CMS/OIS)

**Cc:** Grothe, Kirk A. (CMS/OIS); Oh, Mark U. (CMS/OIS); Van, Hung B. (CMS/OIS); Margush, Doug C. (CMS/OIS); Coutts, Todd (CMS/OIS); Lyles, Darrin V. (CMS/OIS) ([Darrin.Lyles@cms.hhs.gov](mailto:Darrin.Lyles@cms.hhs.gov)); Fletcher, John A. (CMS/OIS)

**Subject:** RE: [NotResp] Checkin

Rebecca and Monique,

I am inclined to say yes we need this fix put in place. The fix is intended to resolve a serious issue where data, which is not a consumers, is showing up in searches and in xqueries. This is starting to result in a high number of security and privacy incidents, and has a public view to it. We should have a quick meeting about this so CMS can make a final determination. Maybe it could come down, if needed, during this weekend to allow for the test?

Also I am not sure why testing can only be done in prod? Can't another set of self-signed certificates be issued to address this? or is it the case where there is not a matching environment to perform the testing in?

Tom

**From:** Fender, Rebecca (CMS/CCSQ)  
**Sent:** Tuesday, November 26, 2013 10:52 AM  
**To:** Schankweiler, Thomas W. (CMS/OIS); Outerbridge, Monique (CMS/OIS); Basavaraju, Venkat (CMS/OIS)  
**Subject:** FW: [REDACTED] NotResp [REDACTED] Checkin  
**Importance:** High

Hi Tom and Monique,

I have serious concerns about this "fix". Every time we do something with the URL we are down for days at SERCO. We can only test this in PROD due to the [REDACTED] NotResp [REDACTED] that goes to EIDM and gets passed to ESD. Can you all let me know if you feel we need to take the risk of SERCO being down for a few days? Trust me when I say there is lots of pressure and focus on SERCO and any downtime they incur due to a CGI fix.

Becky

Becky Fender PMP®

CMS

Cell: [REDACTED] (b)(6)

Office 410-786-1006

**From:** Fender, Rebecca (CMS/CCSQ)  
**Sent:** Tuesday, November 26, 2013 10:48 AM  
**To:** 'O'Mara, Katyanne J (CGI Federal)'; Minze Chien; Venky Natarajan; Basavaraju, Venkat (CMS/OIS); Niranjan Santhamoorthy; [greg.greshman.health@gmail.com](mailto:greg.greshman.health@gmail.com); Nitin Matta; Girish Shetty; Sundar, Raj N (CGI Federal); Thangavelu, Raja (Non-Member); Ivan Vinogradov; Ramamoorthy, Balaji Manikandan (CGI Federal); Anbu, Bala (Non-Member); Cecilio, Sal (CGI Federal); Roche, Jacqueline R. (CMS/CCIIO)  
**Subject:** RE: [REDACTED] NotResp [REDACTED] Checkin

I still do not feel that this is urgent and must happen as a priority. I will discuss with Tom and Monique. I do agree it should happen but I know this will take us down for several days and that simply can't happen at this time. There is NO way to test this other than in prod due to the [REDACTED] NotResp [REDACTED] assertion of their federated login.

Becky Fender PMP®

CMS

Cell: [REDACTED] (b)(6)

Office 410-786-1006

**From:** O'Mara, Katyanne J (CGI Federal) [<mailto:katyanne.omara@cgifederal.com>]  
**Sent:** Tuesday, November 26, 2013 10:45 AM  
**To:** Fender, Rebecca (CMS/CCSQ); Minze Chien; Venky Natarajan; Basavaraju, Venkat (CMS/OIS); Niranjan Santhamoorthy; [greg.greshman.health@gmail.com](mailto:greg.greshman.health@gmail.com); Nitin Matta; Girish Shetty; Sundar, Raj N (CGI Federal); Thangavelu, Raja (Non-Member); Ivan Vinogradov; Ramamoorthy, Balaji Manikandan (CGI Federal); Anbu, Bala (Non-Member);

Cecilio, Sal (CGI Federal); Roche, Jacqueline R. (CMS/CCIIO)

**Subject:** RE: [NotResp] Checkin

Hi Becky,

I understand your concern.

**Defect numbers are in CALT:** artf161121 / artf161124 and this is part of the List of 65, it is N3 which again was identified to better secure [NotResp] If you have further concerns/questions please reach out to Tom Shankweiler.

**To Test:** Go through normal process as an ESW while someone from our security team is in the backend ensures that [NotResp] e. When an ESW closes a completed application) and creates new [NotResp] when they search and choose another application to work on or when they click the "Create Application" link.

Soumya, Manisha, Eddie and others, even Shaina can be part of the front end testing and Balaji will be assigning someone from his security team to work with us in a coordinated testing effort tomorrow to confirm that the [NotResp] are being created and cleared appropriately.

Our Ops and Security team have completed their tasks. Sal will complete his tasks today. I just need confirmation from EIDM team that they made their change. We will be ready for the coordinated test tomorrow.

I will update the document I sent out with this information.

I hope this answers your questions and alleviates your concerns regarding testing. This is about closing the loop on open [NotResp] not changing your workflow or affecting your current workflow it's about making your current [NotResp] more secure.

Thanks,

KO

Katy O'Mara | Manager | Health and Compliance Group | CGI Federal

W: 703-227-6411 | C [NotResp] | [www.cgi.com](http://www.cgi.com)

**From:** Fender, Rebecca (CMS/CCSQ) [<mailto:Rebecca.Fender@cms.hhs.gov>]

**Sent:** Tuesday, November 26, 2013 9:58 AM

**To:** O'Mara, Katyanne J (CGI Federal); Minze Chien; Venky Natarajan; Venkat.Basavaraju; Niranjan Santhamoorthy; [greg.greshman.health@gmail.com](mailto:greg.greshman.health@gmail.com); Nitin Matta; Girish Shetty; Sundar, Raj N (CGI Federal); Thangavelu, Raja (Non-Member); Ivan Vinogradov; Ramamoorthy, Balaji Manikandan (CGI Federal); Anbu, Bala (Non-Member); Cecilio, Sal (CGI Federal); Roche, Jacqueline R. (CMS/CCIIO)

**Subject:** RE: [NotResp] Checkin

I will try to call in later but have a conflicting meeting with NPC and leadership about the notices issues. Sorry. I really do NOT want to move forward with this until I understand how we plan to test and why this is such a rush as well as how it was discovered. As we know from past experience changes like this can keep SERCO down for days and we cannot afford that at this time.

Becky Fender PMP®

CMS

Cell: (b)(6)

Office 410-786-1006

-----Original Appointment-----

**From:** O'Mara, Katyanne J (CGI Federal) [mailto:katyanne.omara@cgifederal.com]

**Sent:** Monday, November 25, 2013 4:20 PM

**To:** O'Mara, Katyanne J (CGI Federal); Minze Chien; Venky Natarajan; Basavaraju, Venkat (CMS/OIS); Niranjana Santhamoorthy; greg.greshman.health@gmail.com; Nitin Matta; Girish Shetty; Sundar, Raj N (CGI Federal); Thangavelu, Raja (Non-Member); Ivan Vinogradov; Ramamoorthy, Balaji Manikandan (CGI Federal); Anbu, Bala (Non-Member); Cecilio, Sal (CGI Federal); Fender, Rebecca (CMS/CCSQ); Roche, Jacqueline R. (CMS/CCIIO)

**Subject:** NotResp: Checkin

**When:** Tuesday, November 26, 2013 10:00 AM-10:30 AM (UTC-05:00) Eastern Time (US & Canada).

**Where:** dial: (b)(6)

Hi Everyone,

I'd like to get an update on the tasks below and ensure we are on target for completion for tomorrow afternoon for testing to begin tomorrow night or Wednesday morning in Test 2.

Detailed Technical Action Items:

**EIDM Team Tasks**

1. Currently EIDM is protecting the URL [https://\(b\)\(6\)](https://(b)(6)) Change the policy to protect the following URL pattern. [\(b\)\(6\)](https://(b)(6))
2. All the header variables remains the same. (NO CHANGES REQUIRED)

NotResp

**FFM Ops Team Tasks**

1. Add the following RP rules for the English

NotResp

2. Restart the Apache RP for the English

### FFM Security Team Tasks

1.	
2.	
3.	
4.	NotResp
5.	
6.	
7.	

### Application Team Tasks

1. Do a ping to [https://\[NotResp\]](https://[NotResp]) every 10 or 15 minutes to keep the [NotResp] active from the main ESD page. (Please get the guidance from Jeremy)
2. Currently in the [NotResp] page when the ESD worker searches for an [NotResp] and clicks on the link, it takes the user to the [NotResp] instead do a HTTP POST to [https://\[NotResp\]](https://[NotResp]). The HTTP POST Parameter should be [NotResp]

Message

**From:** Charest, Kevin (OS/ASA/OCIO/OIS) [Redacted] **NotResp**  
**Sent:** 10/8/2013 9:08:40 PM  
**To:** Schankweiler, Thomas W. (CMS/OIS) [Redacted] **NotResp**  
[Redacted] **NotResp**  
**Subject:** Re: XOC Monday

Tom I was also thinking that in regard to the logs I am also willing to have someone from my staff help work with [Redacted] to resolve any challenges with connecting to the aggregator etc.

Let me know who to contact etc.

Thanks

Kevin

Sent from my iPad

On Oct 8, 2013, at 3:56 PM, "Schankweiler, Thomas W. (CMS/OIS)" <[thomas.schankweiler@cms.hhs.gov](mailto:thomas.schankweiler@cms.hhs.gov)> wrote:  
Kevin,

Sounds good. If they want to send them out of Tuesday I can meet with them and we can work out a strategy for them to help. Here is the address.

XOC Address:

[Redacted] **NotResp**

Tom Schankweiler, CISSP  
Information Security Officer, CCIO  
CMS\OIS\CIISG  
Consumer Information and Insurance Systems Group  
410-786-5956 (Balt. Office, N2-13-22)  
[Redacted] (b)(6) (Mobile)

**From:** Charest, Kevin (OS/ASA/OCIO/OIS)  
**Sent:** Tuesday, October 08, 2013 3:34 PM  
**To:** Fryer, Teresa M. (CMS/OIS); Schankweiler, Thomas W. (CMS/OIS)  
**Cc:** Mellor, Michael (CMS/OIS)  
**Subject:** RE: Update request

Thank you Teresa and Tom for your response.

Teresa would please have someone copy me on these weekly and biweekly reports that are being generated?



Tom I do have a couple of [NotR esp] folks and would like to send one up there to help out for a bit starting next Tuesday. Please let me know the best way to get this person established with your team etc.

Kevin

**From:** Fryer, Teresa M. (CMS/OIS)  
**Sent:** Tuesday, October 08, 2013 2:12 PM  
**To:** Charest, Kevin (OS/ASA/OCIO/OIS)  
**Cc:** Schankweiler, Thomas W. (CMS/OIS); Mellor, Michael (CMS/OIS)  
**Subject:** RE: Update request

Kevin,

From the CISO's perspective, the following update is provided on the monitoring that is being conducted by [NotResp]

AppScan:

- <!--[if !supportLists]--><!--[endif]-->Previously performed scans on 4 [NotR esp] in Pre-Prod, have not conducted rescans as the AppScan team is still waiting for updates on any mitigations before re-scanning those sites.
- <!--[if !supportLists]--><!--[endif]-->healthcare.gov continues to be scanned monthly, the site has been transitioned to the CMS team from the HHS/OS team.
- <!--[if !supportLists]--><!--[endif]-->The CMS team is waiting for any additional URLs that [NotR esp] wants to be scanned to be provided to them for scanning.

Penetration Testing:

- <!--[if !supportLists]--><!--[endif]-->External testing – All border (DMZ) devices including Internet facing web servers will be tested once a week until further notice, with a status report issued each week. Any exploitable vulnerabilities discovered will be immediately reported to the appropriate GTL. The [NotR esp] servers located at the [NotResp] will be tested every two weeks until further notice, with a status report issued for each test. Testing will begin on Monday 9/23.
  - <!--[if !supportLists]--><!--[endif]-->URL testing is being performed as discussed, IP level testing is on hold until the penetration testers are provided DMZ/external IPs to test by [NotResp]
- <!--[if !supportLists]--><!--[endif]-->Internal testing – Testing of the internal devices at [NotResp] would require a [NotResp] or utilize the [NotResp] would require opening firewalls). Given that testing of internal devices is currently being done by another component [NotResp] see little benefit from this line of testing from us.
  - <!--[if !supportLists]--><!--[endif]-->This is still accurate at this time – if [NotR esp] does transition to an alternate [NotR esp] implementation then connectivity needs to be re-examined since the internal pen testers would no longer have access to test.

CSIRT:

- <!--[if !supportLists]--><!--[endif]-->CMS CSIRT is reviewing the daily security reports from the [NotResp] as well as reviewing tickets ad-hoc in [NotR esp] as time permits.

[NotResp] IP360:

- <!--[if !supportLists]--><!--[endif]-->We are currently scanning [NotResp] networks with the [NotR esp] toolset.
- <!--[if !supportLists]--><!--[endif]-->We do plan on beginning to score them officially this month.
- <!--[if !supportLists]--><!--[endif]-->We are running into issues where we are not authenticating to all of their machines – they are aware of these issues, but do not have the time to address everything due to their [NotResp] involvement with the ACA.

- <!--[if !supportLists]--><!--[endif]-->Working on provisioning direct, read-only, access for [NotResp]



- <!--[if !supportLists]--><!--[endif]-->Working on loading a new set of data from [NotResp] environment this week to perform updated reporting and analysis -- [NotResp] is still in the process of providing all the necessary data, we are working with the initial set sent yesterday to try and speed things up as much as possible.

The following update has been provided by Tom:

- <!--[if !supportLists]--><!--[endif]-->Getting status from [Not Res] on the [NotResp]
- <!--[if !supportLists]--><!--[endif]-->Software Code is developed and comment on using the [NotResp] application tool (see attached sample). The developers have direct access to [NotRes] and they check in-and check out their code. The [NotResp] actively reviews the code and also provides comments back to [NotRes]. There are also formal meetings bi-weekly to review top findings that are identified by the team. We have a process guide that describes all of this if you or Kevin are interested in it. In addition, we have a person that regularly tests the site "white-hat" stuff and he provides inputs daily to [NotResp]. If Kevin has a true white-hacker on his team that could be of assistance to us that could prove to be useful.
- <!--[if !supportLists]--><!--[endif]-->As I suggested this morning, opening up a feedback mechanism to allow crowd-sourcing could prove in-valuable. (email attached)

Please let me know if you have any additional questions.

Thanks,

Teresa

**From:** Charest, Kevin (OS/ASA/OCIO/OIS)

**Sent:** Tuesday, October 08, 2013 10:53 AM

**To:** Fryer, Teresa M. (CMS/OIS); Schankweiler, Thomas W. (CMS/OIS)

**Subject:** Update request

Teresa and Tom,

I was wondering if I could get and update from you folks on how you are handling the testing of these code updates that are occurring frequently right now. I know the full court press is on to enhance the throughput for the exchanges but we also have the responsibility to ensure that the code they are putting in place is not introducing significant risk to the entire system.

Also Tom is there anything that I can have my team do to help resolve the issue of getting access to your

[NotResp]

[NotResp]?

Thanks

Kevin

Kevin Charest Ph.D., CISSP, PMP

Chief Information Security Officer

U.S. Department of Health and Human Services

Email: [Kevin.Charest@hhs.gov](mailto:Kevin.Charest@hhs.gov)

[NotResp]

Ofc. 202-690-5548; Mobile:

(b)(6)

Obtained via FOIA by Judicial Watch, Inc.

*"Driving secure solutions through innovation and sustainable business practices"*

Message

**From:** Fryer, Teresa M. (CMS/OIS) [NotResp]  
[NotResp]  
**Sent:** 10/10/2013 4:25:44 PM  
**To:** Charest, Kevin [NotResp]  
Schankweiler, Thomas W. (CMS/OIS) [NotResp]  
[NotResp]  
**CC:** Baitman, Frank (OS/ASA/OCIO) [NotResp]  
[NotResp]  
**Subject:** RE: Admin passwords and insecurity in healthcare.gov

Kevin,

I have received this and will have Jason Ashbaugh follow up with Tom's team on this.

Teresa

**From:** Charest, Kevin (OS/ASA/OCIO/OIS)  
**Sent:** Thursday, October 10, 2013 12:21 PM  
**To:** Fryer, Teresa M. (CMS/OIS); Schankweiler, Thomas W. (CMS/OIS)  
**Cc:** Baitman, Frank (OS/ASA/OCIO)  
**Subject:** FW: Admin passwords and insecurity in healthcare.gov  
**Importance:** High

Teresa and Tom,

As you can see from the email chain below and the article at the Trustedsec site there are a significant number of concerns being raised here and they do appear to be legitimate even partially.

I need for you to review the current status of imbedded developer comment and ensure that they are removed. If – as is implied below, the admin password is something as absurd as what is in the tweet it be immediately changed and should be changed regularly in accordance with security standards and best practices.

Please let me know that you received this message and will be looking into for validation and remediation as soon as possible.

Kevin

Kevin Charest Ph.D., CISSP, PMP  
Chief Information Security Officer  
U.S. Department of Health and Human Services

Email: [Kevin.Charest@hhs.gov](mailto:Kevin.Charest@hhs.gov)

[NotResp]

Ofc. 202-690-5548; Mobile: (b)(6)

*"Driving secure solutions through innovation and sustainable business practices"*

**From:** (b)(6)

**Sent:** Thursday, October 10, 2013 12:12 PM

**To:** Charest, Kevin (OS/ASA/OCIO/OIS)

**Cc:** (b)(6)  
(b)(6)

**Subject:** Admin passwords and insecurity in healthcare.gov

**Importance:** High

Kevin,

NotResp



**TrustedSec** @TrustedSec

2h

Is the Affordable Health Care Website Secure? Probably not.

[trustedsec.com/october\\_2013/a...](http://trustedsec.com/october_2013/a...) #TrustedSec

Collapse

Reply Retweet Favorite More

**22**

RETWEETS

**3**

FAVORITES

(b)(6)

6:40 AM - 10 Oct 13 · Details

(b)(6)

(b)(6)

comments in tha

45m

NotResp

Details

(b)(6)

**Blank Page**

Message

**From:** Linares, George E. (CMS/OIS) [NotResp]  
[NotResp]  
**Sent:** 11/12/2013 8:52:28 PM  
**To:** Feuerberg, Lisa A. (CMS/OIS) [NotResp]  
'hyoud@foregroundsecurity.com' [hyoud@foregroundsecurity.com]; Schankweiler, Thomas W. (CMS/OIS) [NotResp]  
[NotResp]  
**CC:** 'mvillar@ccsin.com' [mvillar@ccsin.com]; 'frank.steiner@noblis.org' [frank.steiner@noblis.org];  
'john.cappelletti@noblis.org' [john.cappelletti@noblis.org]  
**Subject:** Re: Items for Weekly report SUMMARY

We need the revised numbers to complete the report

George Linares

Office of Information Services  
Centers for Medicare & Medicaid Services  
----- Sent using BlackBerry -----

**From:** Feuerberg, Lisa A. (CMS/OIS)  
**Sent:** Tuesday, November 12, 2013 03:49 PM  
**To:** Hank Youd <hyoud@foregroundsecurity.com>; Schankweiler, Thomas W. (CMS/OIS)  
**Cc:** Manuel Villar <mvillar@ccsin.com>; Steiner, Chip <frank.steiner@noblis.org>; Cappelletti, John Danilo  
<john.cappelletti@noblis.org>; Linares, George E. (CMS/OIS)  
**Subject:** RE: Items for Weekly report SUMMARY

Hank & Tom:

We have not yet seen the updates on the incident table (#5). We were expecting it about a ½ hour ago. Please advise.

**Lisa Feuerberg**  
Centers for Medicare & Medicaid Services (CMS)  
Office of Information Services (OIS)  
Information Services Design & Development Group (IHDSG)  
Division of Program Management (DPM)  
☎ 410.786.6840 (O) [ (b)(6) ] (M)  
✉ [lisa.feuerberg@cms.hhs.gov](mailto:lisa.feuerberg@cms.hhs.gov)  
7500 Security Blvd., N3-17-26  
Baltimore, MD 21244-1850

Need more information? Please visit [the OIS website](#).

*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:** Hank Youd [mailto:[hyoud@foregroundsecurity.com](mailto:hyou@foregroundsecurity.com)]  
**Sent:** Tuesday, November 12, 2013 2:42 PM  
**To:** Cappelletti, John Danilo  
**Cc:** Schankweiler, Thomas W. (CMS/OIS); Manuel Villar; Steiner, Chip; Feuerberg, Lisa A.(CMS/OIS)  
**Subject:** Re: Items for Weekly report SUMMARY

Thanks John, I'll review and get back to you.

Thanks,  
Hank

**From:** <Cappelletti>, John Danilo <[john.cappelletti@noblis.org](mailto:john.cappelletti@noblis.org)>  
**Date:** Tuesday, November 12, 2013 2:38 PM  
**To:** Hank Youd <[hyoud@foregroundsecurity.com](mailto:hyou@foregroundsecurity.com)>  
**Cc:** Tom Schankweiler <[thomas.schankweiler@cms.hhs.gov](mailto:thomas.schankweiler@cms.hhs.gov)>, Manuel Villar <[mvillar@ccsin.com](mailto:mvillar@ccsin.com)>, "Steiner, Chip" <[frank.steiner@noblis.org](mailto:frank.steiner@noblis.org)>, "Cappelletti, John Danilo" <[john.cappelletti@noblis.org](mailto:john.cappelletti@noblis.org)>, "Feuerberg, Lisa A.(CMS/OIS) (Lisa.Feuerberg@cms.hhs.gov)" <[Lisa.Feuerberg@cms.hhs.gov](mailto:Lisa.Feuerberg@cms.hhs.gov)>  
**Subject:** RE: Items for Weekly report SUMMARY

Hank,

We have the initial summary as of 9/30 from Manuel (screen shot) and tables of open/closed incidents as of 10/30 and as of 11/7.

Thanks,  
John

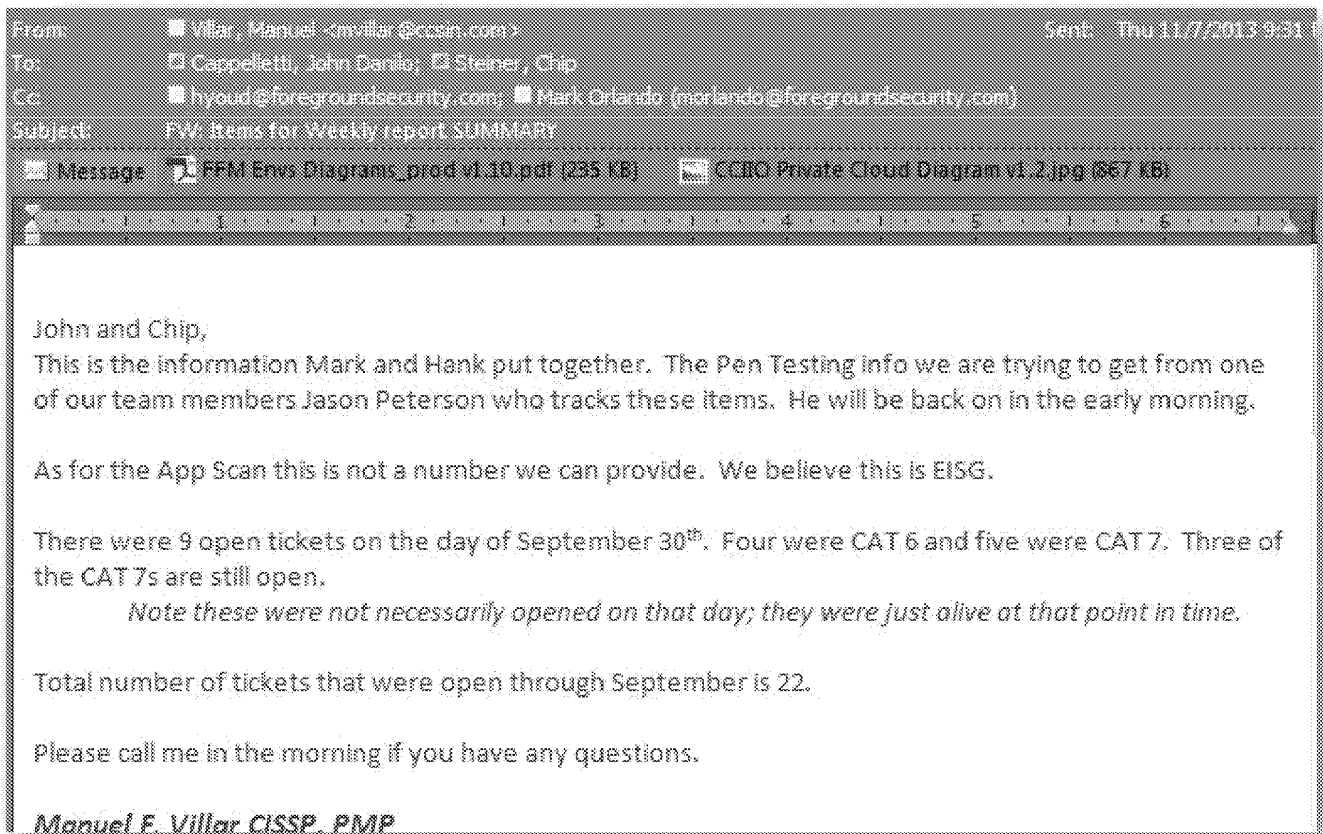


Table for 10/1 through 10/30:

Category	Statistics	Number of Incidents
<b>Category 1</b>	Unauthorized Access: in this category an individual gains logical or physical access without permission to a federal agency network, system, application, data, or other resource.	5 incidents opened/ closed
<b>Category 2</b>	Denial of Service: an attack that successfully prevents or impairs the normal authorized functionality of networks, systems or applications by exhausting resources. This activity includes being the victim or participating in the DoS.	0 incidents opened/closed
<b>Category 3</b>	Malicious Code: Successful installation of malicious software (e.g., virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application. Agencies are NOT required to report malicious logic that has been successfully quarantined by antivirus software.	0 incidents opened/closed
<b>Category 4</b>	Improper Usage: A person violates acceptable computing use policies.	0 incidents opened/closed
<b>Category 5</b>	Scans/Probes/Attempted Access: This category includes any activity that seeks to access or identify a federal agency computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial of service.	0 incidents opened/closed
<b>Category 6 (low level)</b>	Unconfirmed incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review	20 incidents closed (0 based on threat intelligence) 3 incidents opened



Category	Statistics	Number of Incidents
<b>Category 7</b>	Application Findings: Network/System/OS level misconfiguration, defect, or vulnerability	9 incidents opened 1 incident closed
<b>Category 8</b>	System Findings: Network/System/OS level misconfiguration, defect, or vulnerability.	0 incidents opened/closed

Table for 10/31 through 11/7 from Tom:

Category	Statistics	Number of Incidents
<b>Category 1</b>	Unauthorized Access, in this category an individual gains logical or physical access without permission to a federal agency network, system, application, data, or other resource. Includes PII events.	18 incidents opened 2 incidents closed
<b>Category 2</b>	Denial of Service, an attack that successfully prevents or impairs the normal authorized functionality of networks, systems or applications by exhausting resources. This activity includes being the victim or participating in the DoS.	0 incidents opened 0 incidents closed
<b>Category 3</b>	Malicious Code, Successful installation of malicious software (e.g., virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application. Agencies are NOT required to report malicious logic that has been successfully quarantined by antivirus software.	0 incidents opened 1 incidents closed
<b>Category 4</b>	Improper Usage, A person violates acceptable computing use policies.	0 incidents opened 0 incidents closed
<b>Category 5</b>	Scans/Probes/Attempted Access, This category includes any activity that seeks to access or identify a federal agency computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial of service.	1 incidents opened 1 incidents closed
<b>Category 6 (low level)</b>	Unconfirmed incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review	11 incidents closed 5 incidents opened
<b>Category 7</b>	Application Findings, Network/System/OS level misconfiguration, defect, or vulnerability	3 incidents opened 1 incident closed
<b>Category 8</b>	System Findings, Network/System/OS level misconfiguration, defect, or vulnerability.	9 incidents opened 0 incidents closed

John Cappelletti, PMP, CMQ/OE | Manager | Health Innovation  
 703.610.1862 (Office) | (b)(6) (m) | 703.610.1702 (Fax)  
[www.noblis.org](http://www.noblis.org)

**From:** Hank Youd [mailto:[hyou@foregroundsecurity.com](mailto:hyou@foregroundsecurity.com)]

**Sent:** Tuesday, November 12, 2013 2:31 PM

**To:** Cappelletti, John Danilo; Steiner, Chip

**Cc:** Tom Schankweiler; Manuel Villar

**Subject:** Re: Items for Weekly report SUMMARY

All,

My team has revisited this request and has determined that on September 30, there were 15 tickets "alive" that day. There may have been 20 closed in the October summary but that may be due to incidents that were opened and closed in October and not being counted on September 30. Just to be sure, can someone send me the summary that was received, I'd like to verify that data.

Thanks,  
Hank

**From:** <Villar>, Manuel <[mvillar@CCSIN.COM](mailto:mvillar@CCSIN.COM)>

**Reply-To:** Manuel Villar <[mvillar@ccsin.com](mailto:mvillar@ccsin.com)>

**Date:** Friday, November 8, 2013 5:34 PM

**To:** "Cappelletti, John Danilo" <[john.cappelletti@noblis.org](mailto:john.cappelletti@noblis.org)>

**Cc:** Hank Youd <[hyoud@foregroundsecurity.com](mailto:hyoud@foregroundsecurity.com)>, Mark Orlando <[morlando@foregroundsecurity.com](mailto:morlando@foregroundsecurity.com)>, "Feuerberg, Lisa A.(CMS/OIS) (Lisa.Feuerberg@cms.hhs.gov)" <[Lisa.Feuerberg@cms.hhs.gov](mailto:Lisa.Feuerberg@cms.hhs.gov)>, "Steiner, Chip" <[frank.steiner@noblis.org](mailto:frank.steiner@noblis.org)>, Tom Schankweiler <[thomas.schankweiler@cms.hhs.gov](mailto:thomas.schankweiler@cms.hhs.gov)>

**Subject:** RE: Items for Weekly report SUMMARY

That is a very good question. The information my team pulled was directly from CALT so the number should be valid but let my team take a look and we will get back to you.

*Manuel F. Villar CISSP, PMP*  
*Director, Cyber Security*  
*Creative Computing Solutions, Inc. (CCSi)*  
301-309-3123 Office

(b)(6) Cell

----- Original message -----

**From:** "Cappelletti, John Danilo" <[john.cappelletti@noblis.org](mailto:john.cappelletti@noblis.org)>

**Date:** 11/08/2013 17:04 (GMT-05:00)

**To:** "Villar, Manuel" <[mvillar@CCSIN.COM](mailto:mvillar@CCSIN.COM)>

**Cc:** [hyoud@foregroundsecurity.com](mailto:hyoud@foregroundsecurity.com), "Mark Orlando ([morlando@foregroundsecurity.com](mailto:morlando@foregroundsecurity.com))" <[morlando@foregroundsecurity.com](mailto:morlando@foregroundsecurity.com)>, "Feuerberg, Lisa A.(CMS/OIS) ([Lisa.Feuerberg@cms.hhs.gov](mailto:Lisa.Feuerberg@cms.hhs.gov))" <[Lisa.Feuerberg@cms.hhs.gov](mailto:Lisa.Feuerberg@cms.hhs.gov)>, "Steiner, Chip" <[frank.steiner@noblis.org](mailto:frank.steiner@noblis.org)>, "Cappelletti, John Danilo" <[john.cappelletti@noblis.org](mailto:john.cappelletti@noblis.org)>

**Subject:** RE: Items for Weekly report SUMMARY

Manuel,

With regard to Category 6, your email notes that there were 4 open as of 9/30.

The summary of incidents we have through 10/30 has the following for CAT 6: 3 more open, and 20 closed.

Might there have been more CAT 6 open as of 9/30? Am wondering how 20 were closed in October when only 4 + 3 were open.

Thanks,

John

**From:** Villar, Manuel [<mailto:mvillar@ccsin.com>]  
**Sent:** Thursday, November 07, 2013 9:31 PM  
**To:** Cappelletti, John Danilo; Steiner, Chip  
**Cc:** [hyoud@foregroundsecurity.com](mailto:hyoud@foregroundsecurity.com); Mark Orlando ([morlando@foregroundsecurity.com](mailto:morlando@foregroundsecurity.com))  
**Subject:** FW: Items for Weekly report SUMMARY  
**Importance:** High

John and Chip,

This is the information Mark and Hank put together. The Pen Testing info we are trying to get from one of our team members Jason Peterson who tracks these items. He will be back on in the early morning.

As for the App Scan this is not a number we can provide. We believe this is EISG.

There were 9 open tickets on the day of September 30<sup>th</sup>. Four were CAT 6 and five were CAT 7. Three of the CAT 7s are still open.

*Note these were not necessarily opened on that day; they were just alive at that point in time.*

Total number of tickets that were open through September is 22.

Please call me in the morning if you have any questions.

*Manuel F. Villar CISSP, PMP*

*Director, Cyber Security*

Creative Computing Solutions, Inc. (CCSI)

301-309-3123 Office

703-932-3554 Cell

CMS

**Manuel Villar** (Contractor)

703-932-3554 (Direct)

[manuel.villar@cms.hhs.gov](mailto:manuel.villar@cms.hhs.gov)

NotResp

**From:** Mark Orlando [<mailto:morlando@foregroundsecurity.com>]

**Sent:** Thursday, November 07, 2013 6:01 PM

**To:** Villar, Manuel; Hank Youd

**Subject:** Re: Items for Weekly report SUMMARY

**Importance:** High

Guys, here is the information for this week's report. Hank, let's circle back tomorrow on how we can use existing processes (mostly relative to RedSeal and nCircle) to pull this information weekly without adding to our workload. We started doing some things this week that I think will help.

- Fixed Pen Test findings

Assume this will come from EISG based upon their weekly testing.

- Drawing of FFM network (located in **NotResp**)

FFM logical system diagram and cloud network diagram attached.

- **NotResp** updates/findings and items closed

The average host score for this week's findings across all environments was 595, which is an increase from the previous week. The most prevalent vulnerabilities in the environment are for **NotResp** products, which accounted for both the highest number of vulnerabilities and the worst vulnerability scores. This is the first week the **NotResp** leveraged **NotResp** to track vulnerabilities for remediation; closed trackers will be reported beginning next week.

This week, the team opened the following trackers to remediate the most critical system vulnerabilities:

- artf160712
- artf154890
- artf160716
- artf160721

- RedSeal

The Infrastructure risk score remained consistent this week. 6 trackers opened this week for **NotResp** findings within the ACA environment **NotResp** implementation and Production instances. These were primarily low-criticality network vulnerabilities and best practice violations, which have been forwarded to the appropriate support teams for remediation.

- POA&M Dashboard (Attached)

- **NotResp** findings and items closed

Assume this will come from EISG; no AppScan assessments analyzed by the **NotResp** this week.

- **NotResp** application findings and items closed

Trackers opened this week for code and application level vulnerabilities discovered by the **NotResp**

- artf160847, **NotResp**
- artf160927, **NotResp**

- artf146030,
- artf160281,

Obtained via FOIA by Judicial Watch, Inc.

NotResp

**From:** <Villar>, Manuel <[mvillar@CCSIN.COM](mailto:mvillar@CCSIN.COM)>  
**Date:** Thursday, November 7, 2013 4:36 PM  
**To:** Hank Youd <[hyoud@foregroundsecurity.com](mailto:hyouud@foregroundsecurity.com)>  
**Cc:** Mark Orlando <[morlando@foregroundsecurity.com](mailto:morlando@foregroundsecurity.com)>  
**Subject:** Items for Weekly report SUMMARY

From our meeting with Tom and the Noblis guys (report writers) this is the list of information they are looking for;

Bullet list of:

- Fixed Pen Test findings
- Drawing of **NotResp** network (located in **NotResp**)
- **NotResp** updates/findings and items closed
- **NotResp**
- POA&M Dashboard (Attached)
- **NotResp** findings and items closed
- **NotResp** findings and items closed

They would like to know how this is driving business. Don't know if we can provide that.

I will be in a meeting with Tom and **NotResp** for about 30 min and can call if you have any questions

**Manuel F. Villar CISSP, PMP**

**Director, Cyber Security**

Creative Computing Solutions, Inc. (CCSI)  
1901 Research Blvd.Suite 600

Rockville, Maryland 20850

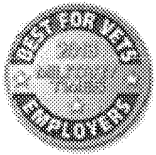
301-309-3123 Office

(b)(6)

Cell

An ISO 9001, 20000-1, 27001 and CMMI Level 3 Company

[www.ccsin.com](http://www.ccsin.com)



**CMS**

**Manuel Villar** (Contractor)

703-932-3554 (Direct)

[manuel.villar@cms.hhs.gov](mailto:manuel.villar@cms.hhs.gov)

NotResp

Please be advised that this transmittal, including any attachments, may be a confidential communication or may otherwise be privileged or proprietary. If you are not the intended recipient, please do not read, use, copy, or re-transmit this communication. Please delete this message and any attachments and notify its sender of the errant delivery. Thank you in advance for your cooperation and assistance.

Please be advised that this transmittal, including any attachments, may be a confidential communication or may otherwise be privileged or proprietary. If you are not the intended recipient, please do not read, use, copy, or re-transmit this communication. Please delete this message and any attachments and notify its sender of the errant delivery. Thank you in advance for your cooperation and assistance.

Please be advised that this transmittal, including any attachments, may be a confidential communication or may otherwise be privileged or proprietary. If you are not the intended recipient, please do not read, use, copy, or re-transmit this communication. Please delete this message and any attachments and notify its sender of the errant delivery. Thank you in advance for your cooperation and assistance.



## Message

**From:** Fryer, Teresa M. (CMS/OIS) [NotResp]  
 [NotResp]  
**Sent:** 10/8/2013 5:02:18 PM  
**To:** Schankweiler, Thomas W. (CMS/OIS) [NotResp]  
 [NotResp] Linares, George E. (CMS/OIS) [NotResp]  
 [NotResp]  
**Subject:** RE: Update request

Below is the update I am providing back to Kevin and I will include Tom's update along with mine. I will be sending this within the half hour, if there are any further updates, please send to be included.

## AppScan:

- Previously performed scans on 4 [NotResp] in Pre-Prod, have not conducted rescans as the AppScan team is still waiting for updates on any mitigations before re-scanning those sites.
- healthcare.gov continues to be scanned monthly, the site has been transitioned to the CMS team from the HHS/OS team.
- The CMS team is waiting for any additional URLs that [NotResp] wants to be scanned to be provided to them for scanning.

## Penetration Testing:

- External testing – All border (DMZ) devices including Internet facing web servers will be tested once a week until further notice, with a status report issued each week. Any exploitable vulnerabilities discovered will be immediately reported to the appropriate GTL. The [NotResp] servers located at the [NotResp] will be tested every two weeks until further notice, with a status report issued for each test. Testing will begin on Monday 9/23.
  - URL testing is being performed as discussed, IP level testing is on hold until the penetration testers are provided DMZ/external IPs to test by [NotResp]
- Internal testing – Testing of the internal devices at [NotResp] would require a [NotResp] or utilize the [NotResp] (would require opening firewalls). Given that testing of internal devices is currently being done by another component [NotResp], I see little benefit from this line of testing from us.
  - This is still accurate at this time – if [NotResp] does transition to an alternate [NotResp] implementation then connectivity needs to be re-examined since the internal pen testers would no longer have access to test.

## CSIRT:

- CMS CSIRT is reviewing the daily security reports from the [NotResp], as well as reviewing tickets ad-hoc in [NotResp] as time permits.

## [NotResp]/IP360:

- We are currently scanning [NotResp] networks with the [NotResp] toolset.
- We do plan on beginning to score them officially this month.
- We are running into issues where we are not authenticating to all of their machines – they are aware of these issues, but do not have the time to address everything due to their involvement with the ACA.

## [NotResp]

- Working on provisioning direct, read-only, access for [NotResp]

- Working on loading a new set of data from [NotResp] environment this week to perform updated reporting and analysis. [NotResp] is still in the process of providing all the necessary data, we are working with the initial set sent yesterday to try and speed things up as much as possible.

**From:** Schankweiler, Thomas W. (CMS/OIS)  
**Sent:** Tuesday, October 08, 2013 11:23 AM  
**To:** Fryer, Teresa M. (CMS/OIS)  
**Cc:** Linares, George E. (CMS/OIS)  
**Subject:** RE: Update request

Getting status from [NotRes] on the [NotResp]

Software Code is developed and comment on using the [NotResp] application tool (see attached sample). The developers have direct access to [NotRes] and they check in-and check out their code. The [NotResp] actively reviews the code and also provides comments back to [NotRes]. There are also formal meetings bi-weekly to review top findings that are identified by the team. We have a process guide that describes all of this if you or Kevin are interested in it. In addition, we have a person that regularly tests the site "white-hat" stuff and he provides inputs daily to [NotRes]. [NotResp] etc. If Kevin has a true white-hacker on his team that could be of assistance to us that could prove to be useful.

As I suggested this morning, opening up a feedback mechanism to allow crowd-sourcing could prove in-valuable.

Tom

**From:** Charest, Kevin (OS/ASA/OCIO/OIS)  
**Sent:** Tuesday, October 08, 2013 10:53 AM  
**To:** Fryer, Teresa M. (CMS/OIS); Schankweiler, Thomas W. (CMS/OIS)  
**Subject:** Update request

Teresa and Tom,

I was wondering if I could get an update from you folks on how you are handling the testing of these code updates that are occurring frequently right now. I know the full court press is on to enhance the throughput for the exchanges but we also have the responsibility to ensure that the code they are putting in place is not introducing significant risk to the entire system.

Also Tom is there anything that I can have my team do to help resolve the issue of getting access to your [NotResp]  
[NotResp]

Thanks

Kevin

Kevin Charest Ph.D., CISSP, PMP  
Chief Information Security Officer  
U.S. Department of Health and Human Services

Email: [Kevin.Charest@hhs.gov](mailto:Kevin.Charest@hhs.gov)

NotResp

Ofc. 202-690-5548; Mobile (b)(6)

*"Driving secure solutions through innovation and sustainable business practices"*

Message

**From:** Schankweiler, Thomas W. (CMS/OIS); [Redacted] **NotResp**  
[Redacted] **NotResp**

**Sent:** 10/8/2013 2:19:02 PM

**To:** Linares, George E. (CMS/OIS); [Redacted] **NotResp**  
[Redacted] **NotResp**; Fryer, Teresa M. (CMS/OIS); [Redacted] **NotResp**  
[Redacted] **NotResp**

**CC:** Ashbaugh, Jason L. (CMS/OIS); [Redacted] **NotResp**  
Oh, Mark U. (CMS/OIS); [Redacted] **NotResp**  
[Redacted] **NotResp**

**Subject:** Security Bug - report form

What are your thoughts about brining something like the links below on-line in support of the marketplace? We would need to go to OC and request the development of the page I think we could get a lot of good input using crowd-sourcing.

<https://www.google.com/appserve/security-bugs/new?rl=pdg6g4inx3w2nu9mpg6qbgad>

<https://www.adobe.com/cfusion/mmform/index.cfm?name=securityform>

Regards,

Tom

Message

**From:** Fryer, Teresa M. (CMS/OIS) [NotResp]  
[NotResp]  
**Sent:** 10/8/2013 6:21:41 PM  
**To:** Schankweiler, Thomas W. (CMS/OIS) [NotResp]  
[NotResp]  
**Subject:** RE: Update request

Okay, I'll let Kevin know.

**From:** Schankweiler, Thomas W. (CMS/OIS)  
**Sent:** Tuesday, October 08, 2013 2:19 PM  
**To:** Fryer, Teresa M. (CMS/OIS)  
**Subject:** RE: Update request

Teresa,

I checked on the [NotResp] connection that Kevin is asking about. We can't make any changes until the furlough is over. Part of the change needs to come from [NotResp] and [NotResp] is short staffed to support this if it is not a urgent business requirement.

Tom

**From:** Fryer, Teresa M. (CMS/OIS)  
**Sent:** Tuesday, October 08, 2013 2:12 PM  
**To:** Charest, Kevin (OS/ASA/OCIO/OIS)  
**Cc:** Schankweiler, Thomas W. (CMS/OIS); Mellor, Michael (CMS/OIS)  
**Subject:** RE: Update request

Kevin,

From the CISO's perspective, the following update is provided on the monitoring that is being conducted by [NotResp]

AppScan:

- Previously performed scans on 4 [NotResp] in Pre-Prod, have not conducted rescans as the AppScan team is still waiting for updates on any mitigations before re-scanning those sites.
- healthcare.gov continues to be scanned monthly, the site has been transitioned to the CMS team from the HHS/OS team.
- The CMS team is waiting for any additional URLs that [NotResp] wants to be scanned to be provided to them for scanning.

Penetration Testing:

- External testing -- All border (DMZ) devices including Internet facing web servers will be tested once a week until further notice, with a status report issued each week. Any exploitable vulnerabilities discovered will be immediately reported to the appropriate GTL. The [NotResp] servers located at the [NotResp] will be tested every two weeks until further notice, with a status report issued for each test. Testing will begin on Monday 9/23.
  - URL testing is being performed as discussed. IP level testing is on hold until the penetration testers are provided DMZ/external IPs to test by [NotResp]

- Internal testing – Testing of the internal devices at [NotResp] would require a [NotResp] or utilize the [NotResp] (would require opening firewalls). Given that testing of internal devices is currently being done by another component [NotResp], I see little benefit from this line of testing from us.
  - This is still accurate at this time – if [NotResp] does transition to an alternate [NotResp] implementation then connectivity needs to be re-examined since the internal pen testers would no longer have access to test.

CSIRT:

- CMS CSIRT is reviewing the daily security reports from the [NotResp] as well as reviewing tickets ad-hoc in [NotResp] as time permits.

[NotResp]

- We are currently scanning [NotResp] networks with the [NotResp] toolset.
- We do plan on beginning to score them officially this month.
- We are running into issues where we are not authenticating to all of their machines – they are aware of these issues, but do not have the time to address everything due to their involvement with the ACA.

[NotResp]

- Working on provisioning direct, read-only, access for [NotResp]
- Working on loading a new set of data from [NotResp] environment this week to perform updated reporting and analysis – [NotResp] is still in the process of providing all the necessary data, we are working with the initial set sent yesterday to try and speed things up as much as possible.

The following update has been provided by Tom:

- Getting status from [NotResp] on the [NotResp]
- Software Code is developed and comment on using the [NotResp] application tool (see attached sample). The developers have direct access to [NotResp] and they check in-and check out their code. The [NotResp] actively reviews the code and also provides comments back to [NotResp]. There are also formal meetings bi-weekly to review top findings that are identified by the team. We have a process guide that describes all of this if you or Kevin are interested in it. In addition, we have a person that regularly tests the site “white-hat” stuff and he provides inputs daily to [NotResp] etc. If Kevin has a true white-hacker on his team that could be of assistance to us that could prove to be useful.
- As I suggested this morning, opening up a feedback mechanism to allow crowd-sourcing could prove invaluable. (email attached)

Please let me know if you have any additional questions.

Thanks,

Teresa

**From:** Charest, Kevin (OS/ASA/OCIO/OIS)

**Sent:** Tuesday, October 08, 2013 10:53 AM

**To:** Fryer, Teresa M. (CMS/OIS); Schankweiler, Thomas W. (CMS/OIS)

**Subject:** Update request

Teresa and Tom,

I was wondering if I could get and update from you folks on how you are handling the testing of these code updates that are occurring frequently right now. I know the full court press is on to enhance the throughput for the exchanges but we also have the responsibility to ensure that the code they are putting in place is not introducing significant risk to the entire system.

Also Tom is there anything that I can have my team do to help resolve the issue of getting access to your

NotResp

NotResp

Thanks

Kevin

Kevin Charest Ph.D., CISSP, PMP  
Chief Information Security Officer  
U.S. Department of Health and Human Services

Email: [Kevin.Charest@hhs.gov](mailto:Kevin.Charest@hhs.gov)

NotResp

Ofc. 202-690-5548; Mobile

(b)(6)

*"Driving secure solutions through innovation and sustainable business practices"*

Message

**From:** Fryer, Teresa M. (CMS/OIS) [NotResp]  
 [NotResp]  
**Sent:** 10/8/2013 6:43:14 PM  
**To:** Charest, Kevin (OS/ASA/OCIO/OIS) [NotResp]  
**CC:** Schankweiler, Thomas W. (CMS/OIS) [NotResp]  
 [NotResp] Mellor, Michael (CMS/OIS) [NotResp]  
**Subject:** RE: Update request

Kevin,

Tom checked on the [NotResp] connection that you were asking about. Part of the change needs to come from our [NotResp] Group and they are short staffed due to the furlough. They can't support any changes until the furlough is over unless there is an urgent business requirement and justification for the change.

Teresa

**From:** Fryer, Teresa M. (CMS/OIS)  
**Sent:** Tuesday, October 08, 2013 2:12 PM  
**To:** Charest, Kevin (OS/ASA/OCIO/OIS)  
**Cc:** Schankweiler, Thomas W. (CMS/OIS); Mellor, Michael (CMS/OIS)  
**Subject:** RE: Update request

Kevin,

From the CISO's perspective, the following update is provided on the monitoring that is being conducted by [NotResp]

AppScan:

- Previously performed scans on 4 [NotResp] in Pre-Prod, have not conducted rescans as the AppScan team is still waiting for updates on any mitigations before re-scanning those sites.
- healthcare.gov continues to be scanned monthly, the site has been transitioned to the CMS team from the HHS/OS team.
- The CMS team is waiting for any additional URLs that [NotResp] wants to be scanned to be provided to them for scanning.

Penetration Testing:

- External testing – All border (DMZ) devices including Internet facing web servers will be tested once a week until further notice, with a status report issued each week. Any exploitable vulnerabilities discovered will be immediately reported to the appropriate GTL. The [NotResp] servers located at the [NotResp] will be tested every two weeks until further notice, with a status report issued for each test. Testing will begin on Monday 9/23.
  - URL testing is being performed as discussed. IP level testing is on hold until the penetration testers are provided DMZ/external IPs to test by [NotResp]
- Internal testing – Testing of the internal devices at [NotResp] would require a [NotResp] or utilize the [NotResp] (would require opening firewalls). Given that testing of internal devices is currently being done by another component (the [NotResp]) I see little benefit from this line of testing from us.
  - This is still accurate at this time – if [NotResp] does transition to an alternate [NotResp] implementation then connectivity needs to be re-examined since the internal pen testers would no longer have access to test.



CSIRT:

- CMS CSIRT is reviewing the daily security reports from the [NotResp] as well as reviewing tickets ad-hoc in [NotResp] as time permits.

[NotResp] IP360:

- We are currently scanning [NotResp] networks with the [NotResp] toolset.
- We do plan on beginning to score them officially this month.
- We are running into issues where we are not authenticating to all of their machines – they are aware of these issues, but do not have the time to address everything due to their involvement with the ACA.

[NotResp]

- Working on provisioning direct, read-only, access for [NotResp]
- Working on loading a new set of data from [NotResp] environment this week to perform updated reporting and analysis. [NotResp] is still in the process of providing all the necessary data, we are working with the initial set sent yesterday to try and speed things up as much as possible.

The following update has been provided by Tom:

- Getting status from [NotResp] on the [NotResp]
- Software Code is developed and comment on using the [NotResp] application tool (see attached sample). The developers have direct access to [NotResp] and they check in-and check out their code. The [NotResp] actively reviews the code and also provides comments back to [NotResp]. There are also formal meetings bi-weekly to review top findings that are identified by the team. We have a process guide that describes all of this if you or Kevin are interested in it. In addition, we have a person that regularly tests the site “white-hat” stuff and he provides inputs daily to [NotResp] etc. If Kevin has a true white-hacker on his team that could be of assistance to us that could prove to be useful.
- As I suggested this morning, opening up a feedback mechanism to allow crowd-sourcing could prove invaluable. (email attached)

Please let me know if you have any additional questions.

Thanks,

Teresa

**From:** Charest, Kevin (OS/ASA/OCIO/OIS)

**Sent:** Tuesday, October 08, 2013 10:53 AM

**To:** Fryer, Teresa M. (CMS/OIS); Schankweiler, Thomas W. (CMS/OIS)

**Subject:** Update request

Teresa and Tom,

I was wondering if I could get and update from you folks on how you are handling the testing of these code updates that are occurring frequently right now. I know the full court press is on to enhance the throughput for the exchanges but we also have the responsibility to ensure that the code they are putting in place is not introducing significant risk to the entire system.

Also Tom is there anything that I can have my team do to help resolve the issue of getting access to your

[NotResp]

[NotResp] ?

Thanks

Kevin

Kevin Charest Ph.D., CISSP, PMP  
Chief Information Security Officer  
U.S. Department of Health and Human Services

Email: [Kevin.Charest@hhs.gov](mailto:Kevin.Charest@hhs.gov)

NotResp

Ofc. 202-690-5548; Mobile (b)(6)

*"Driving secure solutions through innovation and sustainable business practices"*

Message

**From:** Fryer, Teresa M. (CMS/OIS) [NotResp]  
[NotResp]  
**Sent:** 10/8/2013 7:52:21 PM  
**To:** Schankweiler, Thomas W. (CMS/OIS) [NotResp]  
[NotResp]  
**CC:** Linares, George E. (CMS/OIS) [NotResp]  
[NotResp]  
**Subject:** FW: Update request

Tom,

I will leave it up to you as to whether or not you want to provide your daily reports to Kevin.

Teresa

**From:** Charest, Kevin (OS/ASA/OCIO/OIS)  
**Sent:** Tuesday, October 08, 2013 3:34 PM  
**To:** Fryer, Teresa M. (CMS/OIS); Schankweiler, Thomas W. (CMS/OIS)  
**Cc:** Mellor, Michael (CMS/OIS)  
**Subject:** RE: Update request

Thank you Teresa and Tom for your response.

Teresa would please have someone copy me on these weekly and biweekly reports that are being generated?

Tom I do have a couple of [Not Res] folks and would like to send one up there to help out for a bit starting next Tuesday. Please let me know the best way to get this person established with your team etc.

Kevin

**From:** Fryer, Teresa M. (CMS/OIS)  
**Sent:** Tuesday, October 08, 2013 2:12 PM  
**To:** Charest, Kevin (OS/ASA/OCIO/OIS)  
**Cc:** Schankweiler, Thomas W. (CMS/OIS); Mellor, Michael (CMS/OIS)  
**Subject:** RE: Update request

Kevin,

From the CISO's perspective, the following update is provided on the monitoring that is being conducted by [Not Res]:

AppScan:

- Previously performed scans on 4 [NotResp] in Pre-Prod, have not conducted rescans as the AppScan team is still waiting for updates on any mitigations before re-scanning those sites.
- healthcare.gov continues to be scanned monthly, the site has been transitioned to the CMS team from the HHS/OS team.
- The CMS team is waiting for any additional URLs that [NotResp] wants to be scanned to be provided to them for scanning.

Penetration Testing:

- External testing – All border (DMZ) devices including Internet facing web servers will be tested once a week until further notice, with a status report issued each week. Any exploitable vulnerabilities discovered will be immediately reported to the appropriate GTL. The [NotResp] servers located at the [NotResp] will be tested every two weeks until further notice, with a status report issued for each test. Testing will begin on Monday 9/23.
  - URL testing is being performed as discussed, IP level testing is on hold until the penetration testers are provided DMZ/external IPs to test by [NotResp]
- Internal testing – Testing of the internal devices at [NotResp] would require a [NotResp] or utilize the [NotResp] (would require opening firewalls). Given that testing of internal devices is currently being done by another component [NotResp] I see little benefit from this line of testing from us.
  - This is still accurate at this time – if [NotResp] does transition to an alternate [NotResp] implementation then connectivity needs to be re-examined since the internal pen testers would no longer have access to test.

CSIRT:

- CMS CSIRT is reviewing the daily security reports from the [NotResp], as well as reviewing tickets ad-hoc in [NotResp] as time permits.  
[NotResp] IP360:
    - We are currently scanning [NotResp] networks with the [NotResp] toolset.
    - We do plan on beginning to score them officially this month.
    - We are running into issues where we are not authenticating to all of their machines – they are aware of these issues, but do not have the time to address everything due to their involvement with the ACA.
- [NotResp]:
- Working on provisioning direct, read-only, access for [NotResp]
  - Working on loading a new set of data from [NotResp] environment this week to perform updated reporting and analysis – [NotResp] is still in the process of providing all the necessary data, we are working with the initial set sent yesterday to try and speed things up as much as possible.

The following update has been provided by Tom:

- Getting status from [NotResp] in the [NotResp]
- Software Code is developed and comment on using the [NotResp] application tool (see attached sample). The developers have direct access to [NotResp] and they check in-and check out their code. The [NotResp] actively reviews the code and also provides comments back to [NotResp]. There are also formal meetings bi-weekly to review top findings that are identified by the team. We have a process guide that describes all of this if you or Kevin are interested in it. In addition, we have a person that regularly tests the site “white-hat” stuff and he provides inputs daily to [NotResp] etc. If Kevin has a true white-hacker on his team that could be of assistance to us that could prove to be useful.
- As I suggested this morning, opening up a feedback mechanism to allow crowd-sourcing could prove invaluable. (email attached)

Please let me know if you have any additional questions.

Thanks,

Teresa

**From:** Charest, Kevin (OS/ASA/OCIO/OIS)

**Sent:** Tuesday, October 08, 2013 10:53 AM

**To:** Fryer, Teresa M. (CMS/OIS); Schankweiler, Thomas W. (CMS/OIS)

**Subject:** Update request

Teresa and Tom,

I was wondering if I could get an update from you folks on how you are handling the testing of these code updates that are occurring frequently right now. I know the full court press is on to enhance the throughput for the exchanges but we also have the responsibility to ensure that the code they are putting in place is not introducing significant risk to the entire system.

Also Tom is there anything that I can have my team do to help resolve the issue of getting access to your

NotResp

NotResp

Thanks

Kevin

Kevin Charest Ph.D., CISSP, PMP  
Chief Information Security Officer  
U.S. Department of Health and Human Services

Email: [Kevin.Charest@hhs.gov](mailto:Kevin.Charest@hhs.gov)

NotResp

Ofc. 202-690-5548; Mobile: (b)(6)

*"Driving secure solutions through innovation and sustainable business practices"*

Message

**From:** Fryer, Teresa M. (CMS/OIS) [NotResp]  
**Sent:** 10/8/2013 7:56:19 PM  
**To:** Charest, Kevin (OS/ASA/OCIO/OIS) [NotResp]  
 Schankweiler, Thomas W. (CMS/OIS) [NotResp]  
**CC:** Mellor, Michael (CMS/OIS) [NotResp]  
**Subject:** RE: Update request

Kevin, will do. Jason Ashbaugh will copy you on what we do as they are generated.

Thanks,

Teresa

**From:** Charest, Kevin (OS/ASA/OCIO/OIS)  
**Sent:** Tuesday, October 08, 2013 3:34 PM  
**To:** Fryer, Teresa M. (CMS/OIS); Schankweiler, Thomas W. (CMS/OIS)  
**Cc:** Mellor, Michael (CMS/OIS)  
**Subject:** RE: Update request

Thank you Teresa and Tom for your response.

Teresa would please have someone copy me on these weekly and biweekly reports that are being generated?

Tom I do have a couple of [NotResp] folks and would like to send one up there to help out for a bit starting next Tuesday. Please let me know the best way to get this person established with your team etc.

Kevin

**From:** Fryer, Teresa M. (CMS/OIS)  
**Sent:** Tuesday, October 08, 2013 2:12 PM  
**To:** Charest, Kevin (OS/ASA/OCIO/OIS)  
**Cc:** Schankweiler, Thomas W. (CMS/OIS); Mellor, Michael (CMS/OIS)  
**Subject:** RE: Update request

Kevin,

From the CISO's perspective, the following update is provided on the monitoring that is being conducted by [NotResp].

AppScan:

- Previously performed scans on 4 [NotResp] in Pre-Prod, have not conducted rescans as the AppScan team is still waiting for updates on any mitigations before re-scanning those sites.
- healthcare.gov continues to be scanned monthly, the site has been transitioned to the CMS team from the HHS/OS team.
- The CMS team is waiting for any additional URLs that [NotResp] wants to be scanned to be provided to them for scanning.

Penetration Testing:

- External testing – All border (DMZ) devices including Internet facing web servers will be tested once a week until further notice, with a status report issued each week. Any exploitable vulnerabilities discovered will be immediately reported to the appropriate GTL. The [NotRes] servers located at the [NotResp] will be tested every two weeks until further notice, with a status report issued for each test. Testing will begin on Monday 9/23.
  - URL testing is being performed as discussed, IP level testing is on hold until the penetration testers are provided DMZ/external IPs to test by [NotResp]
- Internal testing – Testing of the internal devices a [NotResp] would require [NotResp] or utilize the [NotResp] (would require opening firewalls). Given that testing of internal devices is currently being done by another component (the [NotResp]), I see little benefit from this line of testing from us.
  - This is still accurate at this time – if [NOTK.esn] does transition to an alternate [NOTK.esn] implementation then connectivity needs to be re-examined since the internal pen testers would no longer have access to test.

CSIRT:

- CMS CSIRT is reviewing the daily security reports from the [NotResp] as well as reviewing tickets ad-hoc in [NOTK.esn] as time permits.

[NotResp]/IP360:

- We are currently scanning [NotResp] networks with the [NotRes] toolset.
- We do plan on beginning to score them officially this month.
- We are running into issues where we are not authenticating to all of their machines – they are aware of these issues, but do not have the time to address everything due to their involvement with the ACA.

[NotResp]

- Working on provisioning direct, read-only, access for [NotResp]
- Working on loading a new set of data from [NotResp] environment this week to perform updated reporting and analysis – [NotResp] is still in the process of providing all the necessary data, we are working with the initial set sent yesterday to try and speed things up as much as possible.

The following update has been provided by Tom:

- Getting status from [NOTK.Res] on the [NotResp]
- Software Code is developed and comment on using the [NotResp] application tool (see attached sample). The developers have direct access to [NOTK.esn] and they check in-and check out their code. The [NotResp] actively reviews the code and also provides comments back to [NOTK.Res]. There are also formal meetings bi-weekly to review top findings that are identified by the team. We have a process guide that describes all of this if you or Kevin are interested in it. In addition, we have a person that regularly tests the site “white-hat” stuff and he provides inputs daily to [NotResp] etc. If Kevin has a true white-hacker on his team that could be of assistance to us that could prove to be useful.
- As I suggested this morning, opening up a feedback mechanism to allow crowd-sourcing could prove invaluable. (email attached)

Please let me know if you have any additional questions.

Thanks,

Teresa

**From:** Charest, Kevin (OS/ASA/OCIO/OIS)

**Sent:** Tuesday, October 08, 2013 10:53 AM

**To:** Fryer, Teresa M. (CMS/OIS); Schankweiler, Thomas W. (CMS/OIS)

**Subject:** Update request

Teresa and Tom,

I was wondering if I could get an update from you folks on how you are handling the testing of these code updates that are occurring frequently right now. I know the full court press is on to enhance the throughput for the exchanges but we also have the responsibility to ensure that the code they are putting in place is not introducing significant risk to the entire system.

Also Tom is there anything that I can have my team do to help resolve the issue of getting access to your

NotResp

NotResp

Thanks

Kevin

Kevin Charest Ph.D., CISSP, PMP  
Chief Information Security Officer  
U.S. Department of Health and Human Services

Email: [Kevin.Charest@hhs.gov](mailto:Kevin.Charest@hhs.gov)

NotResp

Ofc. 202-690-5548; Mobile (b)(6)

*"Driving secure solutions through innovation and sustainable business practices"*



Message

---

**From:** Schankweiler, Thomas W. (CMS/OIS) (b)(5)  
(b)(5)  
**Sent:** 11/8/2013 1:44:17 AM  
**To:** Boulanger, Jennifer L. (CMS) (b)(5)  
(b)(5)  
**Subject:** Re: Compilation of statements/ background on security

Jennifer,

In case you do not hear from them, they do appear correct. I was at the table for a majority of these discussions. HHS still needs to publish the privacy impact assessments on their web site. I am hoping it will be completed next week.

Tom

**From:** Fryer, Teresa M. (CMS/OIS)  
**Sent:** Thursday, November 07, 2013 07:54 PM  
**To:** Boulanger, Jennifer L. (CMS); Trenkle, Tony (CMS/OIS); Schankweiler, Thomas W. (CMS/OIS); Tagalicod, Robert (CMS/OEM); Franey, Maribel R. (CMS/OEM)  
**Cc:** Nelson, David J. (CMS/OEM); Chao, Henry (CMS/OIS); Aronson, Lauren (CMS/OL); Bradley, Tasha (CMS/OC)  
**Subject:** RE: Compilation of statements/ background on security

I believe Maribel Franey is out of the office, try Theo Wills.

---

**From:** Boulanger, Jennifer L. (CMS)  
**Sent:** Thursday, November 07, 2013 7:39 PM  
**To:** Trenkle, Tony (CMS/OIS); Fryer, Teresa M. (CMS/OIS); Schankweiler, Thomas W. (CMS/OIS); Tagalicod, Robert (CMS/OEM); Franey, Maribel R. (CMS/OEM)  
**Cc:** Nelson, David J. (CMS/OEM); Chao, Henry (CMS/OIS); Aronson, Lauren (CMS/OL); Bradley, Tasha (CMS/OC)  
**Subject:** RE: Compilation of statements/ background on security  
Thanks! + Rob and Maribel

Rob and Maribel, I left you off the original note. Would you take a look at the privacy statement below and give me any comments tomorrow morning?

Thanks so much!

Jennifer

**From:** Boulanger, Jennifer L. (CMS)  
**Sent:** Thursday, November 07, 2013 06:15 PM  
**To:** Trenkle, Tony (CMS/OIS); Fryer, Teresa M. (CMS/OIS); Schankweiler, Thomas W. (CMS/OIS)  
**Cc:** Nelson, David J. (CMS/OEM); Chao, Henry (CMS/OIS); Aronson, Lauren (CMS/OL); Bradley, Tasha (CMS/OC)  
**Subject:** FW: Compilation of statements/ background on security

Tony and Tom,

Below is a compilation of statements that have been made on security that ASPA is working on. Could you please look at these and give me any comments ASAP? I am worried about the statements about mitre. Is there anyone else who

should comment? We are being asked to provide comments by 9am and I am sorry for the overly short timeframe. (anything you can give me is appreciated – even if after 9am.)

Thanks so much!

Jennifer

**Draft/ Pre-Decisional/ Not for Distribution**

### **Security: Clearing up the Facts**

**Statement from HHS spokesperson:** “The privacy and security of consumers personal information is a top priority for us. When consumers fill out their online marketplace applications they can trust that the information that they are providing is protected by stringent security standards. Security testing happens on an ongoing basis using industry best practices to appropriately safeguard consumers personal information.

**(b)(5)**

**(b)(5)**

#### **From CMS Data Hub Fact Sheet:**

CMS developed the marketplace systems consistent with federal statutes, guidelines and industry standards that ensure the security, privacy, and integrity of systems and the data that flows through them. All of CMS’ marketplace systems of records are subject to the Privacy Act of 1974, the Computer Security Act of 1987, and the Federal Information Security Management Act of 2002. These systems must also comply with various rules and regulations promulgated by HHS, the Office of Management and Budget, the Department of Homeland Security, and the National Institute of Standards and Technology.

#### **Excerpts from Secretary Sebelius: Senate Finance Committee Hearing, 11/6/13**

- **(b)(5)**
- “Well, I share your concerns about individual privacy. And I would say the site was developed with the highest standards in mind. It is FISMA (ph) certified, which is the federal standard. It meets the NIST standards.”
- **(b)(5)**

#### **ADDITIONAL BACKGROUND AS NEEDED:**

##### **FISMA authority: How does this work?**

- The six-month authorization to operate is a determination that the Federally Facilitated Marketplace (FFM) is FISMA compliant.
- All authorities to operate (ATOs) are required to have a termination date under FISMA guidance. There is currently a six-month authority to operate in place for the FFM. Security testing is happening on an ongoing

basis using industry best practices and, as required in the ATO, technical experts are undertaking a number of strategies to mitigate risks. The FFM's six-month authority to operate is fully FISMA compliant.

(b)(5)

(b)(5)

**Privacy: How are you making sure that you are protecting the privacy of applicants when it comes to personal information?**

- Applications are retained by the FFM in case there is an appeal of the eligibility determination. The security/privacy of the FFM meets the Federal standards for the maintenance of personally identifiable information.
- After attesting to having authority to apply on a family or household member's behalf, individuals filing an application online may submit information about those household members that is subject to verification. The Exchange verifies whether the information submitted by the applicant, such as name, address, or social security number, is consistent with information from data sources, and if not, the individual is asked to provide additional information to resolve the inconsistency. The Exchange does not show information about family or household members received from data sources to the application filer during the application process.
- After consultation with OMB, which is statutorily charged with overseeing and assisting agencies in implementing the Privacy Act, HHS & SSA determined that this use of information for verification purposes is authorized by the Privacy Act as a "routine use."
- The Privacy Act authorizes agencies to disclose agency records as a "routine use" when doing so is "compatible with the purpose for which the information was collected." Because eligibility determinations are among the reasons for which the records are collected, the records' use by the Exchange constitutes a routine use. This is consistent with many other previously established routine uses in which information is provided for purposes of eligibility determinations in health maintenance or other government benefit programs, such as Medicaid, Social Security or LIHEAP.

(b)(5)

**(b)(5)**

(b)(5)

**[i] NIST Guide for Applying the Risk Management Framework to Federal Information Systems (Appendix F, P F-5)**  
**<http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf>**

### **F.3 AUTHORIZATION DECISION DOCUMENT**

The *authorization decision document* transmits the final security authorization decision from the authorizing official to the information system owner or common control provider and other key organizational officials, as appropriate. The authorization decision document contains the following information:

- Authorization decision;
- Terms and conditions for the authorization;
- Authorization termination date; and

- Risk executive (function) input (if provided).

The security *authorization decision* indicates whether the information system is: (i) authorized to operate; or (ii) not authorized to operate. For common controls, the authorization decision means that the controls are approved for *inheritance* by organizational information systems. The *terms and conditions* for the authorization provide a description of any limitations or restrictions placed on the operation of the information system or the implementation of common controls that must be followed by the system owner or common control provider. The *authorization termination date*, established by the authorizing official, indicates when the security authorization expires and reauthorization is required. An authorizing official designated representative prepares the authorization decision document for the authorizing official with authorization recommendations, as appropriate. The authorization decision document is attached to the original authorization package and transmitted to the information system owner or common control provider.<sup>69</sup>

Upon receipt of the authorization decision document and authorization package, the information system owner or common control provider acknowledges and implements the terms and conditions of the authorization and notifies the authorizing official. The information system owner or common control provider retains the original authorization decision document and authorization package.<sup>70</sup> The organization ensures that authorization documents for information systems and for common controls are available to appropriate organizational officials (e.g., information system owners inheriting common controls, the risk executive [function], chief information officers, senior information security officers, information system security officers). The contents of the security authorization documentation, especially information regarding information system vulnerabilities, are: (i) marked and appropriately protected in accordance with federal/organizational policy; and (ii) retained in accordance with the organization's record retention policy. The authorizing official verifies on an ongoing basis, that the terms and conditions established as part of the authorization are being followed by the information system owner or common control provider.

Message

**From:** Schankweiler, Thomas W. (CMS/OIS) **NotResp**  
**NotResp**  
on behalf of Schankweiler, Thomas W. (CMS/OIS)  
**Sent:** 12/5/2013 7:28:56 PM  
**To:** Reinhold, Leslie A. (CMS/OEM) **NotResp**  
**Subject:** RE: HHS Request: IT Response Plans for 2 Tickets

Yes please

**From:** Reinhold, Leslie A. (CMS/OEM)  
**Sent:** Thursday, December 05, 2013 1:43 PM  
**To:** Schankweiler, Thomas W. (CMS/OIS)  
**Subject:** Re: HHS Request: IT Response Plans for 2 Tickets

There was 2 at the bottom of that list are we addressing both?

Sent from my iPhone

On Dec 5, 2013, at 1:01 PM, "Schankweiler, Thomas W. (CMS/OIS)" <[thomas.schankweiler@cms.hhs.gov](mailto:thomas.schankweiler@cms.hhs.gov)> wrote:  
Leslie will need to handle that.

**From:** Alexander, David (CMS/OIS)  
**Sent:** Thursday, December 05, 2013 12:59 PM  
**To:** Schankweiler, Thomas W. (CMS/OIS)  
**Cc:** Ambrosini, Ellen M. (CMS/OEM); Wills, Theodora (CMS/OEM); Reinhold, Leslie A. (CMS/OEM); Fryer, Teresa M. (CMS/OIS)  
**Subject:** RE: HHS Request: IT Response Plans for 2 Tickets

Tom – I hate to be a pain, but these need to be put into the template format (see attached).

Thanks

David Alexander, CISSP

410-786-3001

**From:** Schankweiler, Thomas W. (CMS/OIS)  
**Sent:** Thursday, December 05, 2013 12:33 PM  
**To:** Reinhold, Leslie A. (CMS/OEM); Fryer, Teresa M. (CMS/OIS)  
**Cc:** Ambrosini, Ellen M. (CMS/OEM); Alexander, David (CMS/OIS); Wills, Theodora (CMS/OEM)  
**Subject:** RE: HHS Request: IT Response Plans for 2 Tickets

All,

Here is the write up to close out 25244 in risk vision.

[Data.healthcare.gov](http://Data.healthcare.gov)

11/19 - Socrata investigated their platform for any signs of malicious activity. First, the activity referred to is the public user profile search API which doesn't reveal any private user information that could be exploited. Second, there is no connection or integration between Socrata platform user accounts and healthcare.gov user accounts. They are completely separate. Third, Socrate has been monitoring and there are no indications of any malicious activity targeting the Socrata platform or data.healthcare.gov.

Please close this as a False Positive -99

Thanks,

Tom

**From:** Schankweiler, Thomas W. (CMS/OIS)  
**Sent:** Thursday, December 05, 2013 11:42 AM  
**To:** Reinhold, Leslie A. (CMS/OEM); Fryer, Teresa M. (CMS/OIS)  
**Cc:** Ambrosini, Ellen M. (CMS/OEM); Alexander, David (CMS/OIS); Wills, Theodora (CMS/OEM)  
**Subject:** RE: HHS Request: IT Response Plans for 2 Tickets

The one for Balaji is no the 25244. If that the healthcare.data.gov then I has sent you the threads on that from OC and you were going to write it up.

**From:** Reinhold, Leslie A. (CMS/OEM)  
**Sent:** Thursday, December 05, 2013 11:39 AM  
**To:** Fryer, Teresa M. (CMS/OIS)  
**Cc:** Ambrosini, Ellen M. (CMS/OEM); Alexander, David (CMS/OIS); Schankweiler, Thomas W. (CMS/OIS); Reinhold, Leslie A. (CMS/OEM); Wills, Theodora (CMS/OEM)  
**Subject:** Re: HHS Request: IT Response Plans for 2 Tickets

Tom it's on that printout we looked at on Tuesday it's the last 2, the brute force attack that Balagi wrote up and data.gov. I know we discussed the data.gov one. Write up what the deal is with that if we are closing it let me know.

Thanks

On Dec 5, 2013, at 11:33 AM, "Fryer, Teresa M. (CMS/OIS)" <[Teresa.Fryer@cms.hhs.gov](mailto:Teresa.Fryer@cms.hhs.gov)> wrote:  
Ellen,

What is #25244, Tom has indicated he does not know what this is and you have indicated that both tickets are for Marketplace.

Teresa

**From:** Ambrosini, Ellen M. (CMS/OEM)  
**Sent:** Wednesday, December 04, 2013 6:58 PM  
**To:** Fryer, Teresa M. (CMS/OIS); Alexander, David (CMS/OIS); Schankweiler, Thomas W. (CMS/OIS)  
**Cc:** Reinhold, Leslie A. (CMS/OEM); Wills, Theodora (CMS/OEM)



**Subject:** HHS Request: IT Response Plans for 2 Tickets

**Importance:** High

Good evening, Teresa-

We met with HHS today and they are requesting several HHS Response Plans on several tickets. Therefore, please complete a Response Plan (template attached) for the below two IT tickets from the Marketplace:

- [NotResp] # 24913 [NotResp] INC000002589982 (see below for status)
- [NotResp] # 25244, N/A [NotResp] ticket as this was entered by CMS IRT.

We will be preparing a Response Plan for several tickets covering an issue regarding potential PII violations and will ask you to review / input the IT section, as necessary.

All of these plans are due to the Department before COB on Friday, December 6<sup>th</sup>. We asked for an extension today and was told that the information is required on Friday.

Please let me know if you have any questions.

Thank you,

*Ellen M. Ambrosini*

*Acting Director, Division of Privacy Policy*

*Privacy Policy Compliance Group, Office of E-Health Standards & Services*

*Centers for Medicare & Medicaid Services*

*7500 Security Boulevard*

*Baltimore, Maryland 21244*

*410-786-6918*

<image001.jpg>

**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:** Schankweiler, Thomas W. (CMS/OIS)

**Sent:** Tuesday, December 03, 2013 1:02 PM

**To:** Reinhold, Leslie A. (CMS/OEM)

**Subject:** Fw: INC000002589982

**From:** Ramamoorthy, Balaji Manikandan (CGI Federal) [mailto:balajimanikandan.ramamoorthy@cgifederal.com]

**Sent:** Tuesday, December 03, 2013 12:31 PM

**To:** Schankweiler, Thomas W. (CMS/OIS); Warren, Kevin (CMS/OIS); Lyles, Darrin V. (CMS/OIS); sbanks@foregroundsecurity.com <sbanks@foregroundsecurity.com>

**Cc:** [redacted]; Martin, Rich (CGI Federal) <Rich.Martin@cgifederal.com>; Promisel, Andrew L (CGI Federal) <andy.promisel@cgifederal.com>; Alford, Justin (CGI Federal) <justin.alford@cgifederal.com>

**Subject:** INC000002589982

Hi Tom,

As discussed here is the write up for the incident # INC000002589982. Please forward it as necessary.

**Issue:**

An authenticated user can craft a malicious script [redacted] against the URL that provides the EligibilityNotice.pdf. If the [redacted] on the system is not truly Unique, this could pose a risk of disclosure to users. Once logged into HealthCare.gov, a user could script [redacted] against the system to retrieve any user's eligibility form.

**Analysis:**

A Proof of Concept was performed by the Marketplace Security Team where user A provided a URL to user B. User B was able to see the EligibilityNotice.pdf for User A.

**Resolution:**

FFM security team have put a code fix in place that will check the meta data of the notices stored in [redacted] and make sure that it is associated with the user who is logged in before it could be downloaded by the user. The meta data for the notice includes the [redacted] and the username. The fix accounts for different roles such as

1. Consumers
2. Agents/Brokers
3. CCR's
4. ESD workers.

The fix has been successfully tested in the lower environments for all these roles and the code has been promoted to the production. The enforcement has not been turned on in production due to the following reasons.

1. Currently the meta data is not populated for the notices stored in [redacted]. All the existing notices have to be updated for the meta data by the data cleanup team. This involves checking the [redacted] for all notices, obtaining the [redacted] and username and populating [redacted] with proper meta data.
2. The development team has to update the code to make sure that any new notice generation is populating the proper meta data going forward.

**Action Items**

We don't have an ETA for these 2 tasks listed above and when the enforcement can be turned on. I have copied Justin Alford (who leads the data cleanup team) and Andy Promisel (who leads the development efforts) in the email as well.

Please let me know if you need more information.

Thanks

Balaji M. Ramamoorthy

**Blank Page**

Message

**From:** Schankweiler, Thomas W. [NotResp]  
 on behalf of Schankweiler, Thomas W. (CMS/OIS)  
**Sent:** 12/6/2013 3:47:36 PM  
**To:** Willard, Adam (CMS/CTR) [NotResp]  
 [NotResp] Youd, Hank (CMS/CTR) [NotResp]  
**CC:** Orlando, Mark (CMS/CTR) [NotResp]  
 [NotResp] Villar, Manuel (CMS/CTR) [NotResp]  
 [NotResp]  
 [NotResp] Warren, Kevin (CMS/OIS)  
 [NotResp]  
 [NotResp] Lyles, Darrin V. (CMS/OIS) [NotResp]  
**Subject:** RE: Incidents Created/Updated

There is a new waiting room area being built that should soon be available (days), where people will be directed to.. When this page comes up, the main site will be blocked for access by Akamai. A consumer will be able to enter their e-mail address and a e-mail blast will be sent letting people know when the site has been returned to service. So this risk should be functionally addressed soon.

**From:** Willard, Adam (CMS/CTR)  
**Sent:** Friday, December 06, 2013 10:36 AM  
**To:** Schankweiler, Thomas W. (CMS/OIS); Youd, Hank (CMS/CTR)  
**Cc:** Orlando, Mark (CMS/CTR); Villar, Manuel (CMS/CTR)  
**Subject:** RE: Incidents Created/Updated

Tom,

Breaking away from the main thread to just discuss the underlying issue.

It is only a matter of time before someone will end up posting a "Security Vulnerability" with text stating something like "Bypass wait times and system down times for healthcare.gov"

If this does occur, then there is the possibility for a malicious user to easily bypass the intention of the wait pages or system down messages. It would be easy to start attacking an already overloaded system.

**Adam Willard** (Contractor)  
 703-354-2229 x513 (Direct)  
 (b)(6) (Mobile)  
[Adam.Willard@cms.hhs.gov](mailto:Adam.Willard@cms.hhs.gov)

**To report a security incident, please contact the:**  
**CMS Marketplace Security Team**  
 Consumer Information & Insurance Systems Group (CIISG)  
 Centers for Medicare & Medicaid Services (CMS)  
 Phone - 703-594-4961 [NotResp] 24/7 coverage)

[NotResp]

DISCLAIMER:

THE INFORMATION CONTAINED IN THIS MESSAGE AND ANY FILE TRANSMITTED WITH IT IS INTENDED ONLY FOR THE USE OF THE INDIVIDUAL OR ENTITY TO WHICH IT IS ADDRESSED AND MAY CONTAIN INFORMATION THAT IS PRIVILEGED, CONFIDENTIAL, AND EXEMPT

FROM DISCLOSURE. Any disclosure, distribution, copying or use of the information by anyone other than the intended recipient, regardless of address or routing, is strictly prohibited. If you have received this message in error, please advise the sender by immediate reply and delete the original message. Personal messages express views solely of the sender and are not attributable to the company.

---

**From:** Schankweiler, Thomas W. (CMS/OIS)

**Sent:** Friday, December 06, 2013 10:17 AM

**To:** Willard, Adam (CMS/CTR); 'dilip.shenoy@cgifederal.com';

NotResp

'lynn.goodrich@cgifederal.com'

**Cc:** Orlando, Mark (CMS/CTR); 'sbanks@foregroundsecurity.com'

**Subject:** Re: Incidents Created/Updated

Yes the bypass is by design with akamai. You can close that one.

**From:** Willard, Adam (CMS/CTR)

**Sent:** Friday, December 06, 2013 10:11 AM

**To:** Shenoy, Dilip (CGI Federal) <dilip.shenoy@cgifederal.com>; Schankweiler, Thomas W. (CMS/OIS);

NotResp

NotResp

lynn.goodrich@cgifederal.com <lynn.goodrich@cgifederal.com>

**Cc:** Orlando, Mark (CMS/CTR); 'sbanks@foregroundsecurity.com' <sbanks@foregroundsecurity.com>

**Subject:** Incidents Created/Updated

New:

INC000002632290

INC000002632338

INC000002632357

INC000002632373

INC000002632383

NotResp

Updated

INC000002629675

INC000002619501

INC000002619250

**Adam Willard** (Contractor)

703-354-2229 x513 (Direct)

(b)(6) Mobile)

Adam.Willard@cms.hhs.gov

**To report a security incident, please contact the:**

**CMS Marketplace Security Team**

Consumer Information & Insurance Systems Group (CIISG)

Centers for Medicare & Medicaid Services (CMS)

Phone - 703-594-4961 (b)(6) (24/7 coverage)

NotResp

DISCLAIMER:

THE INFORMATION CONTAINED IN THIS MESSAGE AND ANY FILE TRANSMITTED WITH IT IS INTENDED ONLY FOR THE USE OF THE INDIVIDUAL OR ENTITY TO WHICH IT IS ADDRESSED AND MAY CONTAIN INFORMATION THAT IS PRIVILEGED, CONFIDENTIAL, AND EXEMPT FROM DISCLOSURE. Any disclosure, distribution, copying or use of the information by anyone other than the intended recipient, regardless of address or routing, is strictly prohibited. If you have received this message in error, please advise the sender by immediate reply and delete the original message. Personal messages express views solely of the sender and are not attributable to the company.

---

**From:** Shenoy, Dilip (CGI Federal) [dilip.shenoy@cgifederal.com]

**Sent:** Friday, December 06, 2013 9:59 AM

**To:** Willard, Adam (CMS/CTR); Schankweiler, Thomas W. (CMS/OIS);

NotResp

**Cc:** Orlando, Mark (CMS/CTR); 'sbanks@foregroundsecurity.com'

**Subject:** RE: Spanish Site Testing

Good morning Adam - I can answer the question. The eligibility notice is in the language selected in the 'communication preferences' section of the application. It is per application, so if you fill in an application in Spanish and choose English as you communication preference, the notice should show up in English. Another application for the same person (different state) with a communication preference of Spanish would show up in Spanish. Hope that helps.

Thanks,  
Dilip

Dilip Shenoy  
Sr Consultant | **CGI Federal** Health & Compliance Security Practice (HCSP) | Desk: 703-272-1264 |  
Email | [Dilip.Shenoy@cgifederal.com](mailto:Dilip.Shenoy@cgifederal.com)

**From:** Willard, Adam (CMS/CTR) [<mailto:Adam.Willard@cms.hhs.gov>]  
**Sent:** Friday, December 06, 2013 9:26 AM  
**To:** Schankweiler, Thomas W. (CMS/OIS); [NotResp]  
**Cc:** Orlando, Mark (CMS/CTR); 'sbanks@foregroundsecurity.com'  
**Subject:** RE: Spanish Site Testing

Current INC tickets have been updated with their information from last night.  
INC000002619250  
INC000002629675  
INC000002619501

I still have to create new tickets for other issues.

Btw, are all eligibility notices in English? Even the one's created through the spanish site (I didn't get much sleep)?

**Adam Willard** (Contractor)  
703-354-2229 x513 (Direct)  
[b)(6)] (Mobile)  
[Adam.Willard@cms.hhs.gov](mailto:Adam.Willard@cms.hhs.gov)

**To report a security incident, please contact the:**  
**CMS Marketplace Security Team**  
Consumer Information & Insurance Systems Group (CIISG)  
Centers for Medicare & Medicaid Services (CMS)  
Phone - 703-594-4961 d [NotResp] (24/7 coverage)  
[NotResp]

DISCLAIMER:

THE INFORMATION CONTAINED IN THIS MESSAGE AND ANY FILE TRANSMITTED WITH IT IS INTENDED ONLY FOR THE USE OF THE INDIVIDUAL OR ENTITY TO WHICH IT IS ADDRESSED AND MAY CONTAIN INFORMATION THAT IS PRIVILEGED, CONFIDENTIAL, AND EXEMPT FROM DISCLOSURE. Any disclosure, distribution, copying or use of the information by anyone other than the intended recipient, regardless of address or routing, is strictly prohibited. If you have received this message in error, please advise the sender by immediate reply and delete the original message. Personal messages express views solely of the sender and are not attributable to the company.

---

**From:** Schankweiler, Thomas W. (CMS/OIS)  
**Sent:** Friday, December 06, 2013 8:38 AM  
**To:** Willard, Adam (CMS/CTR); [NotResp]  
**Cc:** Orlando, Mark (CMS/CTR); 'sbanks@foregroundsecurity.com'  
**Subject:** RE: Spanish Site Testing

The front end (Spanish or English) technically should not matter. We only need one open incident per "type"

Thanks,

Tom

**From:** Willard, Adam (CMS/CTR)

**Sent:** Friday, December 06, 2013 8:25 AM

**To:** Schankweiler, Thomas W. (CMS/OIS); [Redacted] NotResp

**Cc:** Orlando, Mark (CMS/CTR); 'sbanks@foregroundsecurity.com'

**Subject:** RE: Spanish Site Testing

I will start putting them in.

There are input validation issues; should those all be tied back to the current INC that deals with the issues identified previously and the issue from the FL user?

**Adam Willard** (Contractor)

703-354-2229 x513 (Direct)

[Redacted] (b)(6) (Mobile)

[Adam.Willard@cms.hhs.gov](mailto:Adam.Willard@cms.hhs.gov)

**To report a security incident, please contact the:**

**CMS Marketplace Security Team**

Consumer Information & Insurance Systems Group (CIISG)

Centers for Medicare & Medicaid Services (CMS)

Phone - 703-594-4961 [Redacted] NotResp (24/7 coverage)

[Redacted] NotResp

DISCLAIMER:

THE INFORMATION CONTAINED IN THIS MESSAGE AND ANY FILE TRANSMITTED WITH IT IS INTENDED ONLY FOR THE USE OF THE INDIVIDUAL OR ENTITY TO WHICH IT IS ADDRESSED AND MAY CONTAIN INFORMATION THAT IS PRIVILEGED, CONFIDENTIAL, AND EXEMPT FROM DISCLOSURE. Any disclosure, distribution, copying or use of the information by anyone other than the intended recipient, regardless of address or routing, is strictly prohibited. If you have received this message in error, please advise the sender by immediate reply and delete the original message. Personal messages express views solely of the sender and are not attributable to the company.

---

**From:** Schankweiler, Thomas W. (CMS/OIS)

**Sent:** Friday, December 06, 2013 8:08 AM

**To:** Willard, Adam (CMS/CTR); [Redacted] NotResp

**Cc:** Orlando, Mark (CMS/CTR); 'sbanks@foregroundsecurity.com'

**Subject:** Re: Spanish Site Testing

They all need to go into remedy, and out of the spreadsheet. Let's talk Monday afternoon. I'll be in Herndon all next week.

**From:** Willard, Adam (CMS/CTR)

**Sent:** Thursday, December 05, 2013 11:20 PM

**To:** [Redacted] NotResp

**Cc:** Schankweiler, Thomas W. (CMS/OIS); Orlando, Mark (CMS/CTR)

**Subject:** Spanish Site Testing

Good evening,

I am continuing to test the Spanish site. However, there are the same issues from the main HC.gov site and new issues. I wanted to see how we are going to proceed with submitting findings. If this is remedy, how quickly will the turn around be for it.

I am tracking primitively in excel currently.

There are some new issues for me also. Here are a few.

On that isn't a security concern is that the

NotResp

I am able to modify information regarding 1 user while logged in as another. Similar to the one I already sent.

The same issues exist with

NotResp

in the UI.

I also took screen shots of some of the pages to maybe assist in identifying the root cause.

EIDM has all the same issues (obviously but needed to state to cover my bases).

1 application I have (due to being able to edit by disabling the stylesheet to edit the application) now has 2 eligibility notices.

There are no backend verifications for the email or telephone numbers on an application.

**Adam Willard** (Contractor)

703-354-2229 x513 (Direct)

(b)(6) Mobile)

[Adam.Willard@cms.hhs.gov](mailto:Adam.Willard@cms.hhs.gov)

**To report a security incident, please contact the:**

**CMS Marketplace Security Team**

Consumer Information & Insurance Systems Group (CIISG)

Centers for Medicare & Medicaid Services (CMS)

Phone - 703-594-4961 or

NotResp

NotResp

DISCLAIMER:

THE INFORMATION CONTAINED IN THIS MESSAGE AND ANY FILE TRANSMITTED WITH IT IS INTENDED ONLY FOR THE USE OF THE INDIVIDUAL OR ENTITY TO WHICH IT IS ADDRESSED AND MAY CONTAIN INFORMATION THAT IS PRIVILEGED, CONFIDENTIAL, AND EXEMPT FROM DISCLOSURE. Any disclosure, distribution, copying or use of the information by anyone other than the intended recipient, regardless of address or routing, is strictly prohibited. If you have received this message in error, please advise the sender by immediate reply and delete the original message. Personal messages express views solely of the sender and are not attributable to the company.



Message

**From:** Schankweiler, Thomas W. (CMS/OIS); [Redacted] NotResp  
[Redacted] NotResp  
**Sent:** 12/6/2013 8:14:17 PM  
**To:** CMS; [Redacted] NotResp  
[Redacted] NotResp  
**Subject:** Fw: Twittter Traffic on DDoS attacks against healthcare.gov

**From:** Cronin, Patrick (CGI Federal) [mailto:Patrick.Cronin@cgifederal.com]  
**Sent:** Friday, December 06, 2013 03:04 PM  
**To:** Lee, Minsu <mlee@akamai.com>; Schankweiler, Thomas W. (CMS/OIS); [Redacted] NotResp  
[Redacted] NotResp  
**Cc:** Hammond, Edward C <ned.hammond@cgi.com>; Oh, Mark U. (CMS/OIS); Van, Hung B. (CMS/OIS); [Redacted] NotResp  
[Redacted] NotResp Booth, Jon G. (CMS/OC); Patel, Ketan (CMS/OC)  
**Subject:** RE: Twittter Traffic on DDoS attacks against healthcare.gov

Hi Minsu,

It takes about half an hour to flip rate limiting on, correct? So if someone were to do repeated gets on our login page at high rates, we'd be down for about 30 minutes right?

Thanks,

*Patrick Cronin*  
Executive Consultant, PMP  
Business Engineering  
12601 Fair Lakes Circle, 10th floor | Fairfax, VA 22033  
Tel: 703.227.6934 | Mobile [Redacted] (b)(6)  
[patrick.cronin@cgifederal.com](mailto:patrick.cronin@cgifederal.com)

**From:** Lee, Minsu [mailto:mlee@akamai.com]  
**Sent:** Friday, December 06, 2013 3:02 PM  
**To:** Cronin, Patrick (CGI Federal); Schankweiler, Thomas W. (CMS/OIS); Customer Care at Akamai  
**Cc:** Hammond, Edward C; mark.oh; Van, Hung B. (CMS/OIS); [Redacted] NotResp booth, jon; Patel, Ketan  
**Subject:** Re: Twittter Traffic on DDoS attacks against healthcare.gov

Yes rate limiting is enabled, however in alert mode. When a rate threshold is exceeded, email alerts will go out to the CMS and Akamai teams, whereby the rate limiting rules can be flipped to deny mode if needed. Akamai's security team is also performing proactive monitoring of potentially malicious traffic as we speak.

Current traffic to the site, both Learn and Marketplace, appear normal for the past 30m. What were the indicators of a potential DDoS attack? Do we have any IPs or ranges to focus on?

(Copying Jon and Ketan for awareness.)

Minsu Lee

Sr. Solutions Architect, Public Sector

Akamai Technologies, Inc.

o. 703.581.6466

c. (b)(6)

**From:** <Cronin>, "Patrick (CGI Federal)" <Patrick.Cronin@cgifederal.com>

**Date:** Friday, December 6, 2013 2:37 PM

**To:** Minsu Lee <mlee@akamai.com>, "Schankweiler, Thomas W. (CMS/OIS)" <thomas.schankweiler@cms.hhs.gov>,  
(b)(6) NotResp

**Cc:** "Hammond, Edward C" <ned.hammond@cgi.com>, "mark.oh" <mark.oh@cms.hhs.gov>, "Van, Hung B. (CMS/OIS)" <Hung.Van@cms.hhs.gov> (b)(6) NotResp

**Subject:** RE: Twittter Traffic on DDoS attacks against healthcare.gov

Hi Minsu,

But if the traffic becomes redirected to origin, can you confirm whether we have rate limiting enabled? I'm concerned if these programs get a little bit smarter and use the login page or registration page that we wouldn't be able to handle the traffic.

Thanks,

Patrick Cronin

Executive Consultant, PMP

Business Engineering

12601 Fair Lakes Circle, 10th floor | Fairfax, VA 22033

Tel: 703.227.6934 | Mobile: (b)(6)

patrick.cronin@cgifederal.com

**From:** Lee, Minsu [mailto:mlee@akamai.com]

**Sent:** Friday, December 06, 2013 2:31 PM

**To:** Cronin, Patrick (CGI Federal); Schankweiler, Thomas W. (CMS/OIS); (b)(6) NotResp

**Cc:** Hammond, Edward C; mark.oh; Van, Hung B. (CMS/OIS); (b)(6) NotResp

**Subject:** Re: Twittter Traffic on DDoS attacks against healthcare.gov

Correction – I was the Akamai rep on the call, and I didn't state that I believed the learn side was under a DDoS attack. I stated that the URL in question, /marketplace/individual/, is delivered from Akamai's NetStorage and can thus absorb a high volume of traffic without risk of outage, as opposed to origin content. Apologies if I wasn't clear.

I am monitoring the traffic and am not observing any abnormal spikes currently. I'll continue to monitor and provide updates as needed.

Minsu Lee

Sr. Solutions Architect, Public Sector

Akamai Technologies, Inc.

o. 703.581.6466

c. (b)(6)

**From:** <Cronin>, "Patrick (CGI Federal)" <Patrick.Cronin@cgifederal.com>

**Date:** Friday, December 6, 2013 2:15 PM

**To:** "Schankweiler, Thomas W. (CMS/OIS)" <thomas.schankweiler@cms.hhs.gov>, Minsu Lee <mlee@akamai.com>,  
[Redacted]

NotResp

**Cc:** "Hammond, Edward C" <ned.hammond@cgi.com>, "mark.oh" <mark.oh@cms.hhs.gov>, "Van, Hung B. (CMS/OIS)" <Hung.Van@cms.hhs.gov>, "Hammond, Edward C" <ned.hammond@cgi.com>

**Subject:** RE: Twittter Traffic on DDoS attacks against healthcare.gov

Hi Tom,

Akamai called into the bridge stating they believe the learn side is under what could be a DDoS attack. I've heard that we haven't yet enabled rate limiting within WAF. If they figure out how to hit origin, we could be vulnerable. I recommend we have Akamai put in place rate limiting to protect our origin servers.

Thanks,

*Patrick Cronin*

Executive Consultant, PMP

Business Engineering

12601 Fair Lakes Circle, 10th floor | Fairfax, VA 22033

Tel: 703.227.6934 | Mobile: [Redacted] (b)(6)

[patrick.cronin@cgifederal.com](mailto:patrick.cronin@cgifederal.com)

**From:** Schankweiler, Thomas W. (CMS/OIS) [<mailto:thomas.schankweiler@cms.hhs.gov>]

**Sent:** Thursday, November 07, 2013 8:47 PM

**To:** Cronin, Patrick (CGI Federal); 'mlee@akamai.com'; [Redacted] NotResp

**Cc:** Hammond, Edward C; Oh, Mark U. (CMS/OIS); Van, Hung B. (CMS/OIS)

**Subject:** Re: Twittter Traffic on DDoS attacks against healthcare.gov

Thanks for the note. This has already been investigated by a couple of parties, and been determined to be a non-threat.

Thanks,

Tom

**From:** Cronin, Patrick (CGI Federal) [<mailto:Patrick.Cronin@cgifederal.com>]

**Sent:** Thursday, November 07, 2013 07:48 PM

**To:** mlee@akamai.com <mlee@akamai.com>; [Redacted] NotResp

**Cc:** Schankweiler, Thomas W. (CMS/OIS); Hammond, Edward C <ned.hammond@cgi.com>; Oh, Mark U. (CMS/OIS); Van, Hung B. (CMS/OIS)

**Subject:** Twittter Traffic on DDoS attacks against healthcare.gov

I monitor twitter feeds for healthcare.gov and noticed people posting DDoS attacks against the site. From what it looks like, they're going after the netstorage portions of the site. Your security team may want to watch and possible see if rate limiting needs to be adjusted as I suspect these attacks could mature and overwhelm origin. Here's one of the many articles out there:

<http://www.zdnet.com/new-dos-attack-directed-at-healthcare-gov-7000022940/>

Our code is CMS0.

**Mark**, Ned said he asked about investigating traffic through Akamai yesterday. Did we make any progress on that? Do you know if we have their Web Application Firewall (WAF) product to be able to respond quickly if these attacks mature?

Thanks,

*Patrick Cronin*

**Executive Consultant, PMP**

**Business Engineering**

12601 Fair Lakes Circle, 10th floor | Fairfax, VA 22033

Tel: 703.227.6934 | Mobile: (b)(6)

[patrick.cronin@cgifederal.com](mailto:patrick.cronin@cgifederal.com)

Message

**From:** Schankweiler, Thomas W. [NotResp]  
[NotResp]  
on behalf of Schankweiler, Thomas W. (CMS/OIS)  
**Sent:** 11/5/2013 2:47:50 PM  
**To:** Plummer, Judah (CMS/CTR) [NotResp]  
[NotResp]  
**CC:** Hank Youd (hyoud@foregroundsecurity.com) [hyoud@foregroundsecurity.com]; Warren, Kevin (CMS/OIS)  
(Kevin.Warren@cms.hhs.gov) [NotResp]  
[NotResp] Villar, Manuel (CMS/CTR) [NotResp]  
[NotResp] Villar, Manuel  
[NotResp]  
[NotResp]  
**Subject:** RE: question from CNN about Heritage report

Judah,

Did you send this ticket to the CMS IT Service Desk on Sunday? Have you received an INC### back yet from the service desk?

Tom

**From:** Plummer, Judah (CMS/CTR)  
**Sent:** Sunday, November 03, 2013 6:47 PM  
**To:** Schankweiler, Thomas W. (CMS/OIS)  
**Subject:** RE: question from CNN about Heritage report

The ticket was created, I apologize for the delay. Is there a remedy ticket yet for this or should I submit a request for one?

Thanks,  
Judah

**Judah Plummer** (Contractor)  
703-722-2229 x 524 (Direct)  
(b)(6) (Mobile)  
[judah.plummer@cms.hhs.gov](mailto:judah.plummer@cms.hhs.gov)

[NotResp]

---

**From:** Schankweiler, Thomas W. (CMS/OIS)  
**Sent:** Sunday, November 03, 2013 4:15 PM  
**To:** [NotResp]  
**Cc:** Reinhold, Leslie A. (CMS/OEM); Wills, Theodora (CMS/OEM); Elky, Mark (CMS/OIS); Marantan, James (CMS/OIS)  
**Subject:** FW: question from CNN about Heritage report

To the analyst on duty.

Please open a ticket with the information listed below, populate it as a CAT-1 with PII implications. If you follow the article you will see which citizen reported the incident. Once completed be sure it goes to the CMS IT service desk.

Thanks,

Tom

**From:** Outerbridge, Monique (CMS/OIS)  
**Sent:** Sunday, November 03, 2013 3:50 PM  
**To:** Nelson, David J. (CMS/OEM); Bradley, Tasha (CMS/OC); Grothe, Kirk A. (CMS/OIS); Oh, Mark U. (CMS/OIS); Schankweiler, Thomas W. (CMS/OIS); 'greg.gershman.health@gmail.com'  
**Cc:** Unruh, Patti (CMS/OC)  
**Subject:** RE: question from CNN about Heritage report

CGI just informed us of this problem this afternoon. They are working on a fix now and could be deployed to production in 2 hours. Will keep you posted

**From:** Bradley, Tasha (CMS/OC)  
**Sent:** Sunday, November 03, 2013 3:02 PM  
**To:** Nelson, David J. (CMS/OEM); Outerbridge, Monique (CMS/OIS); Grothe, Kirk A. (CMS/OIS); Oh, Mark U. (CMS/OIS); Schankweiler, Thomas W. (CMS/OIS); 'greg.gershman.health@gmail.com'  
**Cc:** Unruh, Patti (CMS/OC)  
**Subject:** Fw: question from CNN about Heritage report

Hi all- sorry for the Sunday afternoon email. CNN is working on a story based on a Heritage report that a user received another user's eligibility determination.

Is this possible?

If this does happen, what is the procedure to address this?

Are there security measures in place to handle a situation like this?

Is the team aware of any instances that this has occurred?

<http://blog.heritage.org/2013/11/02/exclusive-healthcare-gov-users-warn-of-security-risk-breach-of-privacy/>

**From:** Bataille, Julie (CMS/OC)  
**Sent:** Sunday, November 03, 2013 02:22 PM  
**To:** Bradley, Tasha (CMS/OC)  
**Subject:** Fw: question from CNN about Heritage report

Can u pls take

**From:** Wallace, Gregory [<mailto:gregory.wallace@turner.com>]  
**Sent:** Sunday, November 03, 2013 02:16 PM  
**To:** Bataille, Julie (CMS/OC); Cook, Brian T. (CMS/OC)

**Subject:** question from CNN about Heritage report

Good afternoon,

Checking in for your comment on this Heritage post that a user's information was presented to a different user on HealthCare.gov.

Is this an issue CMS teams are aware of and working on, and are there other instances of this happening?

<http://blog.heritage.org/2013/11/02/exclusive-healthcare-gov-users-warn-of-security-risk-breach-of-privacy/>

Thank you,

Greg Wallace  
CNN  
202-738-3113

Message

**From:** Schankweiler, Thomas W. (CMS/OIS) [NotResp]  
 on behalf of [NotResp]  
 Schankweiler, Thomas W. (CMS/OIS)  
**Sent:** 11/5/2013 5:31:36 PM  
**To:** Outerbridge, Monique (CMS/OIS) [NotResp]  
 [NotResp]  
**CC:** Rhones, Rhonda D. (CMS/OIS) [NotResp]  
 [NotResp] Lyles, Darrin V. (CMS/OIS)  
 (Darrin.Lyles@cms.hhs.gov) [NotResp]  
 [NotResp]  
**Subject:** RE: Admin passwords and insecurity in healthcare.gov

In regards to an update. The issue was resolved almost a month ago. But here is an update to subsequent steps being taken since my last report:

1. [NotResp] has applied the tool to perform minification which is the process of removing all unnecessary characters from source code without changing its functionality.
2. A CR is being created to add Google Captcha to healthcare.gov login page. It will require some testing, and a final business decision if we should implement this now as it adds one more step of complexity to the user login process. With the heat we are getting right now it may be wise to have it tested and ready to go in at a moment's notice, but not turn it on until the consumer experience improves.

Regards,

Tom

**From:** Outerbridge, Monique (CMS/OIS)  
**Sent:** Tuesday, November 05, 2013 12:15 PM  
**To:** Schankweiler, Thomas W. (CMS/OIS)  
**Cc:** Rhones, Rhonda D. (CMS/OIS)  
**Subject:** RE: Admin passwords and insecurity in healthcare.gov

Probably this one.

**From:** Schankweiler, Thomas W. (CMS/OIS)  
**Sent:** Thursday, October 10, 2013 2:09 PM  
**To:** Fryer, Teresa M. (CMS/OIS)  
**Cc:** Ashbaugh, Jason L. (CMS/OIS); Linares, George E. (CMS/OIS); Outerbridge, Monique (CMS/OIS); Oh, Mark U. (CMS/OIS); Chao, Henry (CMS/OIS); Warren, Kevin (CMS/OIS)  
**Subject:** RE: Admin passwords and insecurity in healthcare.gov

Hello all,

Here is the feedback regarding this inquiry.

**Statement:**



CMS [NotResp] acknowledges the feedback by the security community. Analysis of the code and a review of the operational environment has confirmed that the site is secure and operating with low risk to consumers.

The code that has been reposted to Pastebin and commented on by TrustedSec is intended to be available to the public code as it makes the user interface (UI) of the site function. By design, these "resource bundles" contain all of the non-personalized text the user will see throughout the site. There is no admin level ID's or passwords located within the [NotResp] posted on-line. The code base at [NotResp] has also just been queried for strings such as "admin password" and "abc123gov" per the twitter screenshot. No evidence was located that there is admin credential revealed. The person who retweeted with the abc password is just being humorous.

The [NotResp] and the SCA test team does run all of the tools mentioned in the article. A lot of commented code was removed prior to production, and the need to perform [NotResp] is a roadmap item, in fact it is scheduled for release to the [NotResp] environment tonight. Performing minification requires a lot of testing to ensure the application is not broken during [NotResp] compression. . As [NotResp] can be improved they will be release with subsequent builds.

To the other points in the article The marketplace does not use PHP so that is a non-issue. The use of Captcha was considered at one time, but removed to ensure 508-Compliance and to more importantly to remove burden on a consumer as *A Good Consumer Experience* was a design consideration. Also the concept of guessing ID's to see if there is a valid one or not is a known risk. We can look into taking steps at locking down access controls further, but it would negatively effect the user-experience.

Regards,

Tom Schankweiler, CISSP  
Information Security Officer, CCIIO  
CMS\OIS\CIISG  
Consumer Information and Insurance Systems Group  
410-786-5956 (Balt. Office, N2-13-22)  
[Redacted] (b)(6) (Mobile)

**From:** Charest, Kevin (OS/ASA/OCIO/OIS)  
**Sent:** Thursday, October 10, 2013 12:21 PM  
**To:** Fryer, Teresa M. (CMS/OIS); Schankweiler, Thomas W. (CMS/OIS)  
**Cc:** Baitman, Frank (OS/ASA/OCIO)  
**Subject:** FW: Admin passwords and insecurity in healthcare.gov  
**Importance:** High

Teresa and Tom,

As you can see from the email chain below and the article at the Trustedsec site there are a significant number of concerns being raised here and they do appear to be legitimate even partially.

I need for you to review the current status of imbedded developer comment and ensure that they are removed. If – as is implied below, the admin password is something as absurd as what is in the tweet it be immediately changed and should be changed regularly in accordance with security standards and best practices.

Please let me know that you received this message and will be looking into for validation and remediation as soon as possible.

Kevin

Kevin Charest Ph.D., CISSP, PMP  
Chief Information Security Officer  
U.S. Department of Health and Human Services

Email: Kevin.Charest@hhs.gov

NotResp

Ofc. 202-690-5548; Mobile (b)(6)

*“Driving secure solutions through innovation and sustainable business practices”*

**From:** (b)(6)

**Sent:** Thursday, October 10, 2013 12:12 PM

**To:** Charest, Kevin (OS/ASA/OCIO/OIS)

**Cc:** (b)(6)

(b)(6)

**Subject:** Admin passwords and insecurity in healthcare.gov

**Importance:** High

Kevin,

NotResp



**TrustedSec** @TrustedSec

2h

Is the Affordable Health Care Website Secure? Probably not.

trustedsec.com/october\_2013/a... #TrustedSec

Collapse

↩ Reply ↻ Retweet ★ Favorite ... More

**22**

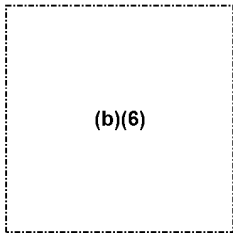
RETWEETS

**3**

FAVORITES

(b)(6)

6:40 AM - 10 Oct 13 · Details



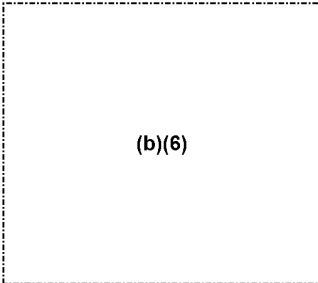
(b)(6)

45m

comments in tha

NotResp

Details



(b)(6)

Message

**From:** Schankweiler, Thomas W. (CMS/OIS) [NotResp]  
on behalf of [NotResp]  
**Sent:** 11/4/2013 8:13:39 PM  
**To:** Boulanger, Jennifer L. (CMS) [NotResp]  
[NotResp]; Unruh, Patti (CMS/OC) [NotResp]  
**CC:** Outerbridge, Monique (CMS/OIS) [NotResp]  
[NotResp]; Lyles, Darrin V. (CMS/OIS) (Darrin.Lyles@cms.hhs.gov) [NotResp]  
[NotResp]  
**Subject:** FW: PII in Analytics tracking - Google

Patti,

FYI... for your 4pm meeting, let me know if it helps.

Tom

**From:** Schankweiler, Thomas W. (CMS/OIS)  
**Sent:** Monday, November 04, 2013 3:12 PM  
**To:** Booth, Jon G. (CMS/OC); 'balajimanikandan.ramamoorthy@cgifederal.com'; 'Jeremy.Jackson@cgifederal.com';  
'jchristopher@blastam.com'; Warren, Kevin (CMS/OIS) (Kevin.Warren@cms.hhs.gov)  
**Cc:** Slavinsky, Gary F. (CMS/OC); Patel, Ketan (CMS/OC); Balasubramanian, Mohanraj (CMS/OC);  
'Keith.Rubin@cgifederal.com'; 'Hemant.Sharma@cgifederal.com'; 'Rich.Martin@cgifederal.com';  
'Paul.Weiss@cgifederal.com'; [NotResp] 'jonathan.keam@cgifederal.com';  
'andrew.brletich@cgifederal.com'; 'Andrew.Newhouse@aquilent.com'; 'Ravi.Mudumby@aquilent.com';  
'Mark.Neuburger@cgifederal.com'; 'catherine.li@akamai.com'; 'mlee@akamai.com'; Reinhold, Leslie A. (CMS/OEM); Wills,  
Theodora (CMS/OEM)  
**Subject:** RE: PII in Analytics tracking - Google

Jon, e.t. all,

I just tried to give you a call. It appears Mr. Simo captured the information posted in his article while in an encrypted session [HTTPS:] and that is why he could view his UserID and the password reset. As Mr. Simo also pointed out in the article that the risk to an individual is low because of the encrypted tunnel. His main point seemed to be that CMS was violating it's own privacy policy as posted on HealthCare.gov which states that no personally identifiable information will be collected by site analytics tools.

I'll update our incident ticket to reflect this information, and we will need to have the CMS privacy weigh in if there was a privacy breach, or just a inadvertent violation of the privacy policy, which has since been corrected. If OESS determines that this is a breach, then they will still need information from the logs showing whose information was transmitted to the analytic tool. Your point that there is only a limited number of people that have access to the analytic tool helps further mitigate the exposure, also Google has stated in earlier messages that they do not have direct access to that information either.

Thanks,

Tom

**From:** Booth, Jon G. (CMS/OC)

**Sent:** Monday, November 04, 2013 11:37 AM

**To:** Schankweiler, Thomas W. (CMS/OIS); 'balajimanikandan.ramamoorthy@cgifederal.com'; 'Jeremy.Jackson@cgifederal.com'; 'jchristopher@blastam.com'

**Cc:** Slavinsky, Gary F. (CMS/OC); Patel, Ketan (CMS/OC); Balasubramanian, Mohanraj (CMS/OC); 'Keith.Rubin@cgifederal.com'; 'Hemant.Sharma@cgifederal.com'; 'Rich.Martin@cgifederal.com'; 'Paul.Weiss@cgifederal.com'; [NotResp] 'jonathan.keam@cgifederal.com'; 'andrew.brletich@cgifederal.com'; 'Andrew.Newhouse@aquilent.com'; 'Ravi.Mudumby@aquilent.com'; 'Mark.Neuburger@cgifederal.com'; 'catherine.li@akamai.com'; 'mlee@akamai.com'

**Subject:** Re: PII in Analytics tracking

Tom,

Here's my take on this — others should feel free to weigh in.

For the data stored in Google Analytics, there was no data exposure. Access to Google Analytics is limited to a very small number of CMS staff and contractors.

However, Google learned about the issue from this article: <http://arstechnica.com/information-technology/2013/10/healthcare-gov-deferred-final-security-check-could-leak-personal-data/>

Given that this was publicly reported, I am not sure how this needs to be handled. OC does not have any insight to this beyond receiving the link to the article from Google.

Thanks,

Jon

Message

**From:** Schankweiler, Thomas W. (CMS/OIS) [NotResp]  
 on behalf of [NotResp]  
 Schankweiler, Thomas W. (CMS/OIS)  
**Sent:** 11/4/2013 8:11:59 PM  
**To:** Booth, Jon G. (CMS/OC) [NotResp]  
 'balajimanikandan.ramamoorthy@cgifederal.com' [NotResp]  
 'Jeremy.Jackson@cgifederal.com' [Jeremy.Jackson@cgifederal.com]; 'jchristopher@blastam.com'  
 '[jchristopher@blastam.com]; Warren, Kevin (CMS/OIS) (Kevin.Warren@cms.hhs.gov) [NotResp]  
 [NotResp]  
**CC:** Slavinsky, Gary F. (CMS/OC) [NotResp]  
 Patel, Ketan (CMS/OC) [NotResp]  
 Balasubramanian, Mohanraj (CMS/OC) [NotResp]  
 [NotResp] [Keith.Rubin@cgifederal.com]  
 '[Keith.Rubin@cgifederal.com]; 'Hemant.Sharma@cgifederal.com' [Hemant.Sharma@cgifederal.com];  
 'Rich.Martin@cgifederal.com' [Rich.Martin@cgifederal.com]; 'Paul.Weiss@cgifederal.com'  
 '[Paul.Weiss@cgifederal.com]; [NotResp]  
 'jonathan.keam@cgifederal.com' [jonathan.keam@cgifederal.com]; 'andrew.brletich@cgifederal.com'  
 '[andrew.brletich@cgifederal.com]; 'Andrew.Newhouse@aquilent.com' [Andrew.Newhouse@aquilent.com];  
 'Ravi.Mudumby@aquilent.com' [Ravi.Mudumby@aquilent.com]; 'Mark.Neuburger@cgifederal.com'  
 '[Mark.Neuburger@cgifederal.com]; 'catherine.li@akamai.com' [catherine.li@akamai.com]; 'mlee@akamai.com'  
 '[mlee@akamai.com]; Reinhold, Leslie A. (CMS/OEM) [NotResp]  
 [NotResp] [Wills, Theodora (CMS/OEM)] [NotResp]  
 [NotResp]  
**Subject:** RE: PII in Analytics tracking - Google

Jon, e.t. all,

I just tried to give you a call. It appears Mr. Simo captured the information posted in his article while in an encrypted session [HTTPS:] and that is why he could view his UserID and the password reset. As Mr. Simo also pointed out in the article that the risk to an individual is low because of the encrypted tunnel. His main point seemed to be that CMS was violating it's own privacy policy as posted on HealthCare.gov which states that no personally identifiable information will be collected by site analytics tools.

I'll update our incident ticket to reflect this information, and we will need to have the CMS privacy weigh in if there was a privacy breach, or just a inadvertent violation of the privacy policy, which has since been corrected. If [NotResp] determines that this is a breach, then they will still need information from the logs showing whose information was transmitted to the analytic tool. Your point that there is only a limited number of people that have access to the analytic tool helps further mitigate the exposure, also Google has stated in earlier messages that they do not have direct access to that information either.

Thanks,

Tom

**From:** Booth, Jon G. (CMS/OC)  
**Sent:** Monday, November 04, 2013 11:37 AM

**To:** Schankweiler, Thomas W. (CMS/OIS); 'balajimanikandan.ramamoorthy@cgifederal.com'; 'Jeremy.Jackson@cgifederal.com'; 'jchristopher@blastam.com'

**Cc:** Slavinsky, Gary F. (CMS/OC); Patel, Ketan (CMS/OC); Balasubramanian, Mohanraj (CMS/OC); 'Keith.Rubin@cgifederal.com'; 'Hemant.Sharma@cgifederal.com'; 'Rich.Martin@cgifederal.com'; 'Paul.Weiss@cgifederal.com'; [REDACTED] NotResp; 'jonathan.keam@cgifederal.com'; 'andrew.brletich@cgifederal.com'; 'Andrew.Newhouse@aquilent.com'; 'Ravi.Mudumby@aquilent.com'; 'Mark.Neuburger@cgifederal.com'; 'catherine.li@akamai.com'; 'mlee@akamai.com'

**Subject:** Re: PII in Analytics tracking

Tom,

Here's my take on this — others should feel free to weigh in.

For the data stored in Google Analytics, there was no data exposure. Access to Google Analytics is limited to a very small number of CMS staff and contractors.

However, Google learned about the issue from this article: <http://arstechnica.com/information-technology/2013/10/healthcare-gov-deferred-final-security-check-could-leak-personal-data/>

Given that this was publicly reported, I am not sure how this needs to be handled. OC does not have any insight to this beyond receiving the link to the article from Google.

Thanks,

Jon

**From:** <Schankweiler>, Thomas Schankweiler BB <[thomas.schankweiler@cms.hhs.gov](mailto:thomas.schankweiler@cms.hhs.gov)>

**Date:** Monday, November 4, 2013 at 11:30 AM

**To:** Balaji Ramamoorthy <[balajimanikandan.ramamoorthy@cgifederal.com](mailto:balajimanikandan.ramamoorthy@cgifederal.com)>, Jeremy Jackson <[Jeremy.Jackson@cgifederal.com](mailto:Jeremy.Jackson@cgifederal.com)>, "'jchristopher@blastam.com'" <[jchristopher@blastam.com](mailto:jchristopher@blastam.com)>

**Cc:** "Slavinsky, Gary F. (CMS/OC)" <[Gary.Slavinsky@cms.hhs.gov](mailto:Gary.Slavinsky@cms.hhs.gov)>, Jon Booth <[jon.booth@cms.hhs.gov](mailto:jon.booth@cms.hhs.gov)>, Ketan Patel BB <[Ketan.Patel@cms.hhs.gov](mailto:Ketan.Patel@cms.hhs.gov)>, "Balasubramanian, Mohanraj (CMS/OC)" <[Mohanraj.Balasubramanian@cms.hhs.gov](mailto:Mohanraj.Balasubramanian@cms.hhs.gov)>, Keith Rubin <[Keith.Rubin@cgifederal.com](mailto:Keith.Rubin@cgifederal.com)>, "'Hemant.Sharma@cgifederal.com'" <[Hemant.Sharma@cgifederal.com](mailto:Hemant.Sharma@cgifederal.com)>, Rich Martin <[Rich.Martin@cgifederal.com](mailto:Rich.Martin@cgifederal.com)>, Paul Weiss <[Paul.Weiss@cgifederal.com](mailto:Paul.Weiss@cgifederal.com)>, [REDACTED] NotResp

[REDACTED] NotResp, "'jonathan.keam@cgifederal.com'" <[jonathan.keam@cgifederal.com](mailto:jonathan.keam@cgifederal.com)>, <[jonathan.keam@cgifederal.com](mailto:jonathan.keam@cgifederal.com)>, "'andrew.brletich@cgifederal.com'" <[andrew.brletich@cgifederal.com](mailto:andrew.brletich@cgifederal.com)>, "Andrew.Newhouse@aquilent.com" <[Andrew.Newhouse@aquilent.com](mailto:Andrew.Newhouse@aquilent.com)>, Ravi Mudumby <[Ravi.Mudumby@aquilent.com](mailto:Ravi.Mudumby@aquilent.com)>, "'Mark.Neuburger@cgifederal.com'" <[Mark.Neuburger@cgifederal.com](mailto:Mark.Neuburger@cgifederal.com)>, "'catherine.li@akamai.com'" <[catherine.li@akamai.com](mailto:catherine.li@akamai.com)>, Minsu Lee <[mlee@akamai.com](mailto:mlee@akamai.com)>

**Subject:** Re: PII in Analytics tracking

I also need to know before it is purged, if there was an exposure of PII, and if so whose data was exposed so that cms can take appropriate breach notification process, or is there no exposure.

Tom

**From:** Ramamoorthy, Balaji Manikandan (CGI Federal) [<mailto:balajimanikandan.ramamoorthy@cgifederal.com>]

**Sent:** Monday, November 04, 2013 11:26 AM

**To:** Jackson, Jeremy (CGI Federal) <[Jeremy.Jackson@cgifederal.com](mailto:Jeremy.Jackson@cgifederal.com)>; Joe Christopher <[jchristopher@blastam.com](mailto:jchristopher@blastam.com)>  
**Cc:** Slavinsky, Gary F. (CMS/OC); Booth, Jon G. (CMS/OC); Patel, Ketan (CMS/OC); Balasubramanian, Mohanraj (CMS/OC); Rubin, Keith (CGI Federal) <[Keith.Rubin@cgifederal.com](mailto:Keith.Rubin@cgifederal.com)>; Sharma, Hemant (CGI Federal) <[Hemant.Sharma@cgifederal.com](mailto:Hemant.Sharma@cgifederal.com)>; Martin, Rich (CGI Federal) <[Rich.Martin@cgifederal.com](mailto:Rich.Martin@cgifederal.com)>; Weiss, Paul (CGI Federal) <[Paul.Weiss@cgifederal.com](mailto:Paul.Weiss@cgifederal.com)>; [NotResp]; Keam, Jonathan (Non-Member) <[jonathan.keam@cgifederal.com](mailto:jonathan.keam@cgifederal.com)>; Brletich, Andrew (Non-Member) <[andrew.brletich@cgifederal.com](mailto:andrew.brletich@cgifederal.com)>; Newhouse, Andrew <[Andrew.Newhouse@aquilent.com](mailto:Andrew.Newhouse@aquilent.com)>; Mudumby, Ravi (<[Ravi.Mudumby@aquilent.com](mailto:Ravi.Mudumby@aquilent.com)>); Neuburger, Mark (CGI Federal) <[Mark.Neuburger@cgifederal.com](mailto:Mark.Neuburger@cgifederal.com)>; catherine.li@akamai.com <[catherine.li@akamai.com](mailto:catherine.li@akamai.com)>; Lee, Minsu <[mlee@akamai.com](mailto:mlee@akamai.com)>; Schankweiler, Thomas W. (CMS/OIS)  
**Subject:** RE: PII in Analytics tracking

Hi Joe,

I am following up on the conversation from last week. Can you please let this thread know about the status of purging the data at Google.

Thanks

Balaji M. Ramamoorthy

**From:** Jackson, Jeremy (CGI Federal)

**Sent:** Thursday, October 31, 2013 8:10 PM

**To:** Joe Christopher

**Cc:** slavinsky, gary; booth, jon; Patel, Ketan; balasubramanian, mohanraj; Rubin, Keith (CGI Federal); Sharma, Hemant (CGI Federal); Martin, Rich (CGI Federal); Weiss, Paul (CGI Federal); Ramamoorthy, Balaji Manikandan (CGI Federal); [NotResp] Keam, Jonathan (Non-Member); Brletich, Andrew (Non-Member); Newhouse, Andrew; Mudumby, Ravi (<[Ravi.Mudumby@aquilent.com](mailto:Ravi.Mudumby@aquilent.com)>); Neuburger, Mark (CGI Federal); catherine.li@akamai.com; Lee, Minsu

**Subject:** RE: PII in Analytics tracking

Hey Guys,

Coming out of our call this afternoon we discovered there were a number of cookies that are unsecured on Healthcare.gov. A best practice would be to enforce [NotResp] where possible. Generally [NotResp] can only be set on cookies that are read server side and [NotResp] could be set on all cookies accessed strictly over https protocols.

We noticed the following external Cookies aren't being set (attached).

- Optimizely
- Chartbeat
- Mix Panel
- Pingdom
- Google Analytics
- Learn side Cookies
- Marketplace cookies

Collectively can the folks on this thread help us determine which of these cookies can be made Secure and which can be set to Http only and if possible configure them in order to future proof them from [NotResp] attacks.

Lite Reading:



<http://www.troyhunt.com/2013/03/c-is-for-cookie-h-is-for-hacker.html>

Let us know if you can help with this security effort.

Thanks,

Jeremy Jackson |CGI Federal

**From:** [joe@blastam.com](mailto:joe@blastam.com) [<mailto:joe@blastam.com>] **On Behalf Of** Joe Christopher

**Sent:** Thursday, October 31, 2013 11:22 AM

**To:** Jackson, Jeremy (CGI Federal)

**Cc:** slavinsky, gary; booth, jon; Patel, Ketan; balasubramanian, mohanraj; Rubin, Keith (CGI Federal); Sharma, Hemant (CGI Federal); Martin, Rich (CGI Federal); Weiss, Paul (CGI Federal); Ramamoorthy, Balaji Manikandan (CGI Federal);

NotResp

**Subject:** Re: PII in Analytics tracking

Hi Jeremy,

That's actually in the window that I am unavailable. If that is the only time, let me know and I'll move what I need to around.

Thanks,



**Joe Christopher**  
Director of Analytics

**Blast Analytics & Marketing**

Analytics & Search Marketing | San Francisco and Roseville, CA  
office: (916) 724-6701 | direct: (916) 724-6715

[www.blastam.com](http://www.blastam.com) | [www.twitter.com/blastam](https://twitter.com/blastam) | [www.blastam.com/blog](http://www.blastam.com/blog)

From Blast Analytics & Marketing



Clickstream data and ownership for Google Analytics.

Learn more: [www.CLICKSTREAMR.com](http://www.CLICKSTREAMR.com)

On Thu, Oct 31, 2013 at 8:20 AM, Jackson, Jeremy (CGI Federal) <[Jeremy.Jackson@cgifederal.com](mailto:Jeremy.Jackson@cgifederal.com)> wrote:

Thanks Joe,

3-3:30 works so I will setup a call for then.

Jeremy Jackson |CGI Federal

**From:** [joe@blastam.com](mailto:joe@blastam.com) [mailto:[joe@blastam.com](mailto:joe@blastam.com)] **On Behalf Of** Joe Christopher

**Sent:** Thursday, October 31, 2013 11:03 AM

**To:** Jackson, Jeremy (CGI Federal)

**Cc:** slavinsky, gary; booth, jon; Patel, Ketan; balasubramanian, mohanraj; Rubin, Keith (CGI Federal); Sharma, Hemant (CGI Federal); Martin, Rich (CGI Federal); Weiss, Paul (CGI Federal); Ramamoorthy, Balaji Manikandan (CGI Federal);

NotResp

**Subject:** Re: PII in Analytics tracking

Hi Jeremy,

Gary and I are on a call right now and can jump onto another call immediately if you like. I am available any time today except 1pm-3:30pm ET.

Thanks,



**Joe Christopher**

Director of Analytics

**Blast Analytics & Marketing**

Analytics & Search Marketing | San Francisco and Roseville, CA  
office: (916) 724-6701 | direct: (916) 724-6715

[www.blastam.com](http://www.blastam.com) | [www.twitter.com/blastam](http://www.twitter.com/blastam) | [www.blastam.com/blog](http://www.blastam.com/blog)

From Blast Analytics & Marketing



Clickstream data and ownership for Google Analytics.

Learn more: [www.CLICKSTREAMR.com](http://www.CLICKSTREAMR.com)

On Thu, Oct 31, 2013 at 7:56 AM, Jackson, Jeremy (CGI Federal) <[Jeremy.Jackson@cgifederal.com](mailto:Jeremy.Jackson@cgifederal.com)> wrote:

Hey Joe,

I received an email chain you forwarded from Google citing an issue with the one of the account reset functionalities containing the users account name in the URL. We are taking steps to remove this functionality from the links.

In the meantime I wanted to setup a meeting with you and Gary along with the other folks in this email to analyze the impacts and possible removal of any metrics associated with this data.

Let us know when a good time to meet is and we will setup a call.

Thank you,

Jeremy Jackson |Manager | CGI Federal | Health and Compliance Group | T: 571-328-6974 | C

(b)(6)

**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.

Message

**From:** Schankweiler, Thomas W. (CMS/OIS) [NotResp]  
 on behalf of [NotResp]  
**Sent:** 12/3/2013 1:34:22 PM  
**To:** Coutts, Todd (CMS/OIS) [NotResp]  
 [NotResp] Garner, John R. (CMS/CMCS) [NotResp]  
 [NotResp] Michael Finkel  
 [mfinkel@qssinc.com]  
**CC:** Grothe, Kirk A. (CMS/OIS) [NotResp]  
 [NotResp] Outerbridge, Monique (CMS/OIS) [NotResp]  
 [NotResp] Lyles, Darrin V. (CMS/OIS)  
 (Darrin.Lyles@cms.hhs.gov) [NotResp]  
 [NotResp] Oh, Mark U. (CMS/OIS) [NotResp]  
 [NotResp] Van, Hung B. (CMS/OIS) [NotResp]  
 [NotResp] Kane, David  
 (CMS/OIS) (David.Kane@cms.hhs.gov) [NotResp]  
 [NotResp]  
**BCC:** Chao, Henry (CMS/OIS) [NotResp]  
**Subject:** RE: ESW Session Management Checkin

Todd, Chip, and Mike

Can we get this coordinated for implementation tonight or on Wed at the latest? Which includes coordination with SERCO.

We have security testing beginning on Monday for FFM and SERCO, and it would be ideal if this fix was in place. We also have a number of open items with the department and DHS which are awaiting this fix action to go in place.

Thanks,

Tom

**From:** Fender, Rebecca (CMS/CCSQ)  
**Sent:** Tuesday, November 26, 2013 7:18 PM  
**To:** Schankweiler, Thomas W. (CMS/OIS)  
**Subject:** RE: ESW Session Management Checkin

Let me know if you need anything else. I'm not opposed to any direction but I do want it coordinated and I do want to make sure leadership isn't upset and frustrated if SERCO goes down. Honestly if I was picking between the two I would pick to fix the PII. It's a broader issue in my book. Just my humble opinion.

Becky Fender PMP®

CMS

Cell: (b)(6)

Office 410-786-1006

CMS000989

**From:** Schankweiler, Thomas W. (CMS/OIS)

**Sent:** Tuesday, November 26, 2013 6:57 PM

**To:** Fender, Rebecca (CMS/CCSQ); Outerbridge, Monique (CMS/OIS); Basavaraju, Venkat (CMS/OIS)

**Cc:** Grothe, Kirk A. (CMS/OIS); Oh, Mark U. (CMS/OIS); Van, Hung B. (CMS/OIS); Margush, Doug C. (CMS/OIS); Coutts, Todd (CMS/OIS); Lyles, Darrin V. (CMS/OIS); Fletcher, John A. (CMS/OIS)

**Subject:** RE: ESW Session Management Checkin

Here is my concern. This change will also effect the way consumers pull data. If we launch and we get a drove of people show up on the 30th and their are presented with exposure of PII, we will have a very bad situation on our hands. So now we are faced with the possibility that Serco could be down for days, when it MUST be up, and the possibility of exposing PII and experiencing a new round of political attacks.

I think if we coordinate decisively that we can all make this work. It would mean identifying a roll-back plan, and implementing the changes on Friday morning, testing by SERCO, and rolling-back quickly if it is not successful. I am not sure what all would need to happen to make this happen, but I think we need to launch on the 30th with a reduced risk of PII exposure; that should be the goal.

I'll be on the 9pm call, and hope maybe we can talk about this near the conclusion of the call.

Thanks,

Tom

---

**From:** Fender, Rebecca (CMS/CCSQ)

**Sent:** Tuesday, November 26, 2013 6:28 PM

**To:** Schankweiler, Thomas W. (CMS/OIS); Outerbridge, Monique (CMS/OIS); Basavaraju, Venkat (CMS/OIS)

**Cc:** Grothe, Kirk A. (CMS/OIS); Oh, Mark U. (CMS/OIS); Van, Hung B. (CMS/OIS); Margush, Doug C. (CMS/OIS); Coutts, Todd (CMS/OIS); Lyles, Darrin V. (CMS/OIS); Fletcher, John A. (CMS/OIS)

**Subject:** RE: ESW Session Management Checkin

Hi All,

I just had a quick call with Tom. I am attaching a document I asked CGI to put together a few days ago when this first came to my attention. Again, I agree this needs to take place and is very important but each time we do something with URLs/Servers or Logins we are down for many days with Serco. In fact we were down today due to changes EIDM made. We need to make sure our timing is coordinated(across all contractors), we have appropriate resources available, a rollback plan and possibly do it after hours/early morning. Whatever timing is decided, we need to make sure all leadership understands the risks to doing it (taking SERCO down) and not doing it (exposing PII). I'm not sure something prior to the 30<sup>th</sup> and our immediate push to clear RIDPs coordinates well with this effort. I will leave it to the group to make recommendations to leadership on timing and priorities.

**Defect numbers are in CALT:** artf161121 / artf161124 and this is part of the List of 65, it is N3 which again was identified to better secure the sessions for both ESD and CCR. If you have further concerns/questions please reach out to Tom Schankweiler.

**To Test:** Go through normal process as an ESW while someone from our security team is in the backend ensures that new sessions go to Layer 7 and L7 clears out old sessions (ie. When an ESW closes a completed application) and creates new sessions when they search and choose another application to work on or when they click the "Create Application" link.

Let me know if you have questions.

Becky

Becky Fender PMP®

CMS

Cell: (b)(6)

Office 410-786-1006

**From:** Schankweiler, Thomas W. (CMS/OIS)

**Sent:** Tuesday, November 26, 2013 5:19 PM

**To:** Outerbridge, Monique (CMS/OIS); Basavaraju, Venkat (CMS/OIS); Fender, Rebecca (CMS/CCSQ)

**Cc:** Grothe, Kirk A. (CMS/OIS); Oh, Mark U. (CMS/OIS); Van, Hung B. (CMS/OIS); Margush, Doug C. (CMS/OIS); Coutts, Todd (CMS/OIS); Lyles, Darrin V. (CMS/OIS); Fletcher, John A. (CMS/OIS)

**Subject:** RE: ESW Session Management Checkin

Did this get resolved today? I can participate in a call later tonight.

Tom

**From:** Schankweiler, Thomas W. (CMS/OIS)

**Sent:** Tuesday, November 26, 2013 12:47 PM

**To:** Fender, Rebecca (CMS/CCSQ); Outerbridge, Monique (CMS/OIS); Basavaraju, Venkat (CMS/OIS)

**Cc:** Grothe, Kirk A. (CMS/OIS); Oh, Mark U. (CMS/OIS); Van, Hung B. (CMS/OIS); Margush, Doug C. (CMS/OIS); Coutts, Todd (CMS/OIS); Lyles, Darrin V. (CMS/OIS) ([Darrin.Lyles@cms.hhs.gov](mailto:Darrin.Lyles@cms.hhs.gov)); Fletcher, John A. (CMS/OIS)

**Subject:** RE: ESW Session Management Checkin

Rebecca and Monique,

I am inclined to say yes we need this fix put in place. The fix is intended to resolve a serious issue where data, which is not a consumers, is showing up in searches and in xqueries. This is starting to result in a high number of security and privacy incidents, and has a public view to it. We should have a quick meeting about this so CMS can make a final determination. Maybe it could come down, if needed, during this weekend to allow for the test?

Also I am not sure why testing can only be done in prod? Can't another set of self-signed certificates be issued to address this? or is it the case where there is not a matching environment to perform the testing in?

Tom

**From:** Fender, Rebecca (CMS/CCSQ)

**Sent:** Tuesday, November 26, 2013 10:52 AM

**To:** Schankweiler, Thomas W. (CMS/OIS); Outerbridge, Monique (CMS/OIS); Basavaraju, Venkat (CMS/OIS)

**Subject:** FW: ESW Session Management Checkin

**Importance:** High

Hi Tom and Monique,

I have serious concerns about this "fix". Every time we do something with the URL we are down for days at SERCO. We can only test this in PROD due to the federated SAML that goes to EIDM and gets passed to ESD. Can you all let me

know if you feel we need to take the risk of SERCO being down for a few days? Trust me when I say there is lots of pressure and focus on SERCO and any downtime they incur due to a CGI fix.

Becky

**Becky Fender PMP®**

CMS

Cell (b)(6)

Office 410-786-1006

**From:** Fender, Rebecca (CMS/CCSQ)

**Sent:** Tuesday, November 26, 2013 10:48 AM

**To:** 'O'Mara, Katyanne J (CGI Federal)'; Minze Chien; Venky Natarajan; Basavaraju, Venkat (CMS/OIS); Niranjana Santhamoorthy; [greg.greshman.health@gmail.com](mailto:greg.greshman.health@gmail.com); Nitin Matta; Girish Shetty; Sundar, Raj N (CGI Federal); Thangavelu, Raja (Non-Member); Ivan Vinogradov; Ramamoorthy, Balaji Manikandan (CGI Federal); Anbu, Bala (Non-Member); Cecilio, Sal (CGI Federal); Roche, Jacqueline R. (CMS/CCIIO)

**Subject:** RE: ESW Session Management Checkin

I still do not feel that this is urgent and must happen as a priority. I will discuss with Tom and Monique. I do agree it should happen but I know this will take us down for several days and that simply can't happen at this time. There is NO way to test this other than in prod due to the SAML assertion of their federated login.

**Becky Fender PMP®**

CMS

Cell (b)(6)

Office 410-786-1006

**From:** O'Mara, Katyanne J (CGI Federal) [<mailto:katyanne.omara@cgifederal.com>]

**Sent:** Tuesday, November 26, 2013 10:45 AM

**To:** Fender, Rebecca (CMS/CCSQ); Minze Chien; Venky Natarajan; Basavaraju, Venkat (CMS/OIS); Niranjana Santhamoorthy; [greg.greshman.health@gmail.com](mailto:greg.greshman.health@gmail.com); Nitin Matta; Girish Shetty; Sundar, Raj N (CGI Federal); Thangavelu, Raja (Non-Member); Ivan Vinogradov; Ramamoorthy, Balaji Manikandan (CGI Federal); Anbu, Bala (Non-Member); Cecilio, Sal (CGI Federal); Roche, Jacqueline R. (CMS/CCIIO)

**Subject:** RE: ESW Session Management Checkin

Hi Becky,

I understand your concern.

**Defect numbers are in CALT:** artf161121 / artf161124 and this is part of the List of 65, it is N3 which again was identified to better secure the sessions for both ESD and CCR. If you have further concerns/questions please reach out to Tom Shankweiler.

**To Test:** Go through normal process as an ESW while someone from our security team is in the backend ensures that new sessions go to Layer 7 and L7 clears out old sessions (ie. When an ESW closes a completed application) and creates new sessions when they search and choose another application to work on or when they click the "Create Application" link.

Soumya, Manisha, Eddie and others, even Shaina can be part of the front end testing and Balaji will be assigning someone from his security team to work with us in a coordinated testing effort tomorrow to confirm that the sessions are being created and cleared appropriately.

Our Ops and Security team have completed their tasks. Sal will complete his tasks today. I just need confirmation from EIDM team that they made their change. We will be ready for the coordinated test tomorrow.

I will update the document I sent out with this information.

I hope this answers your questions and alleviates your concerns regarding testing. This is about closing the loop on open sessions, not changing your workflow or affecting your current workflow it's about making your current sessions more secure.

Thanks,  
KO

Katy O'Mara | Manager | Health and Compliance Group | CGI Federal  
W: 703-227-6411 | C: (b)(6) | [www.cgi.com](http://www.cgi.com)

**From:** Fender, Rebecca (CMS/CCSQ) [<mailto:Rebecca.Fender@cms.hhs.gov>]  
**Sent:** Tuesday, November 26, 2013 9:58 AM  
**To:** O'Mara, Katyanne J (CGI Federal); Minze Chien; Venky Natarajan; Venkat.Basavaraju; Niranjana Santhamoorthy; [greg.greshman.health@gmail.com](mailto:greg.greshman.health@gmail.com); Nitin Matta; Girish Shetty; Sundar, Raj N (CGI Federal); Thangavelu, Raja (Non-Member); Ivan Vinogradov; Ramamoorthy, Balaji Manikandan (CGI Federal); Anbu, Bala (Non-Member); Cecilio, Sal (CGI Federal); Roche, Jacqueline R. (CMS/CCIIO)  
**Subject:** RE: ESW Session Management Checkin

I will try to call in later but have a conflicting meeting with NPC and leadership about the notices issues. Sorry. I really do NOT want to move forward with this until I understand how we plan to test and why this is such a rush as well as how it was discovered. As we know from past experience changes like this can keep SERCO down for days and we cannot afford that at this time.

Becky Fender PMP®  
CMS  
Cell: (b)(6)  
Office 410-786-1006

-----Original Appointment-----

**From:** O'Mara, Katyanne J (CGI Federal) [<mailto:katyanne.omara@cgifederal.com>]  
**Sent:** Monday, November 25, 2013 4:20 PM  
**To:** O'Mara, Katyanne J (CGI Federal); Minze Chien; Venky Natarajan; Basavaraju, Venkat (CMS/OIS); Niranjana Santhamoorthy; [greg.greshman.health@gmail.com](mailto:greg.greshman.health@gmail.com); Nitin Matta; Girish Shetty; Sundar, Raj N (CGI Federal); Thangavelu, Raja (Non-Member); Ivan Vinogradov; Ramamoorthy, Balaji Manikandan (CGI Federal); Anbu, Bala (Non-Member); Cecilio, Sal (CGI Federal); Fender, Rebecca (CMS/CCSQ); Roche, Jacqueline R. (CMS/CCIIO)  
**Subject:** ESW Session Management Checkin



**When:** Tuesday, November 26, 2013 10:00 AM-10:30 AM (UTC-05:00) Eastern Time (US & Canada).

**Where:** dial: (b)(6)

Hi Everyone,

I'd like to get an update on the tasks below and ensure we are on target for completion for tomorrow afternoon for testing to begin tomorrow night or Wednesday morning in Test 2.

Detailed Technical Action Items:

NotResp

2. All the header variables remains the same. (NO CHANGES REQUIRED)

USERROLE

CSRUSERID

FIRSTNAME

MIDDLENAME

LASTNAME

**FFM Ops Team Tasks**

1. Add the following RP rules for the English

NotResp

2. Restart the Apache RP for the English

**FFM Security Team Tasks**

NotResp

**Application Team Tasks**

1. Do a ping to NotResp every 10 or 15 minutes to keep the EIDM session active from the main ESD page. (Please get the guidance from Jeremy)

NotResp

## Message

**From:** Schankweiler, Thomas W. (CMS/OIS) [NotResp]  
 on behalf of [NotResp]  
 Schankweiler, Thomas W. (CMS/OIS)  
**Sent:** 12/3/2013 3:23:43 PM  
**To:** Warren, Kevin (CMS/OIS) [NotResp]  
 [NotResp] Howard, Jacqueline Y. (CMS/OIS) [NotResp]  
 [NotResp]  
**CC:** Hank Youd (hyoud@foregroundsecurity.com) [hyoud@foregroundsecurity.com]  
**Subject:** RE: Security Items that Need Attention

Hank,

Try this. Click on Consoles, then Incident Management

**BMC REMEDY IT SERVICE MANAGEMENT** Welcome, THOMAS W. SCHANKWEILER Close Help bmcsoftware

[View Broadcast](#) **Overview Console**

**Functions**  
**Consoles**  
 IT Home Page  
**Incident Management**  
 Problem Management  
 Change Management  
 Release Management  
 Asset Management  
 Contract Management  
 Software Asset Management  
 Approval Console  
 ROI Console  
 CMDB

Company: [ ] View By: All My Groups

Console List  
 Create View Print Search For Ticket

Showing 1 - 20 of 20 Page: 1 Preferences

Incident ID	Parent Name	Impact Type	Severity	Assigned	Assigned To
INC000002530000		Incident	Medium	vSOC	KEVIN WARR
INC000002583050		Incident	Medium	vSOC	LESLIE A RE
INC000002583827		Incident	Medium	vSOC	KEVIN WARR
INC000002580982		Incident	Medium	vSOC	KEVIN WARR
INC000002591251		Incident	Medium	vSOC	KEVIN WARR
INC000002595237		Incident	Medium	vSOC	
INC000002610890		Incident	Medium	vSOC	George Grayst
INC000002610985		Incident	Medium	vSOC	George Grayst
INC000002610986		Incident	Medium	vSOC	George Grayst
INC000002620017		Incident	Medium	vSOC	George Grayst
INC000002620036		Incident	Medium	vSOC	George Grayst
INC000002620064		Incident	Medium	vSOC	George Grayst
INC000002620102		Incident	Medium	vSOC	George Grayst
INC000002620118		Incident	Medium	vSOC	George Grayst
INC000002620133		Incident	Medium	vSOC	George Grayst
INC000002620145		Incident	Medium	vSOC	George Grayst
INC000002620153		Incident	Medium	vSOC	George Grayst
INC000002620163		Incident	Medium	vSOC	George Grayst
INC000002620167		Incident	Medium	vSOC	George Grayst
INC000002620178		Incident	Medium	vSOC	George Grayst

NotResp

That should give you this screen where you can see all the items in the queue.

**BMC REMEDY IT SERVICE MANAGEMENT - Incident Management**

Current mode: Search

Logout Help Home

Welcome, THOMAS W. SCHANKWEILER

**Incident Console**

Company: [Dropdown] View By: All My Groups

Incidents

Create View Print Quick Actions Add To Watch

Showing 1 - 50 of 63 Page 1

Priority	Status	Assigned	Target D.
Medium	Assigned	KEVIN WARREN	
Medium	Assigned		
Medium	Assigned	LESLIE A. REINHOLD	
Medium	Pending	KEVIN WARREN	
Medium	Pending	KEVIN WARREN	
Medium	In Progress	KEVIN WARREN	
Medium	Assigned		
Medium	In Progress	Reed Erickson	
Medium	In Progress	Reed Erickson	

**Incident Detail and Fields**

Create View Report Show Time

Showing 1 - 2 of 2 Page 1

Type	Summary	Submit Date
General Information	Notified Security of this ticket	10/8/2013 11:30:01 AM
General Information	CSIRT EVENT: CAT 9 Investigation	10/8/2013 10:33:13 AM

**Incident Details:**

- Status Reason: Monitoring Incident
- Assigned Group: vSOC
- Reported Date: 10/8/2013 9:53:08 AM
- Customer: CSIRT, CSIRT
- Notes: From Orlando Mark (CMS/CTR) Sent Sunday October
- Service:

**From:** Warren, Kevin (CMS/OIS)  
**Sent:** Tuesday, December 03, 2013 9:40 AM  
**To:** Howard, Jacqueline Y. (CMS/OIS)  
**Cc:** Schankweiler, Thomas W. (CMS/OIS); Hank Youd (hyoud@foregroundsecurity.com)  
**Subject:** Security Items that Need Attention

Jacqueline,

Some of our team members are still experiencing problems with **NotResp** and access to our security queue. All the members of Marketplace **NotResp** team require read/write access. Let me know if you need any information from me.

Thanks in advance.

Kevin Warren | Centers for Medicare and Medicaid Services (CMS) | Office of Information Services (OIS) | Consumer Information and Insurance Systems Group (CIISG) | 7700 Wisconsin Ave **(b)(6)** Bethesda, Maryland | 301.492.4381 (O)

**From:** Youd, Hank (CMS/CTR)  
**Sent:** Tuesday, December 03, 2013 9:23 AM

**To:** Schankweiler, Thomas W. (CMS/OIS); Warren, Kevin (CMS/OIS)

**Cc:** Villar, Manuel (CMS/CTR)

**Subject:** RE: Security Items that Need Attention

UPDATE,

Correction, we can get to a search page to search ticket numbers but the Incident Management page is empty. Very odd that in order to see anything, it has to be manually search on.

Thanks,

Hank

**From:** Youd, Hank (CMS/CTR)

**Sent:** Tuesday, December 03, 2013 9:14 AM

**To:** Schankweiler, Thomas W. (CMS/OIS); Warren, Kevin (CMS/OIS)

**Cc:** Villar, Manuel (CMS/CTR)

**Subject:** RE: Security Items that Need Attention

Tom,

We are still having remedy issues, I finally got in but I can only see tickets that are related to my CMS account. I don't see any queues that are IR related. Boden sees the same thing so there must be some permissions that need to be granted so we can see the correct queues.

Thanks,

Hank

**From:** Schankweiler, Thomas W. (CMS/OIS)

**Sent:** Tuesday, December 03, 2013 8:52 AM

**To:** Youd, Hank (CMS/CTR); Warren, Kevin (CMS/OIS)

**Cc:** Villar, Manuel (CMS/CTR)

**Subject:** FW: Security Items that Need Attention

Kevin and Hank,

We need to work on this in the afternoon.

Kevin you setup a meeting from noon-1pm please.

Hank, in preparation for the meeting I need a report (spreadsheet or something) of what these remedy incidents are and if they are currently open or closed.

Thanks,

Tom

**From:** Coutts, Todd (CMS/OIS)

**Sent:** Tuesday, November 26, 2013 3:48 PM

**To:** Schankweiler, Thomas W. (CMS/OIS); Kane, David (CMS/OIS); Michael Finkel

**Cc:** Warren, Kevin (CMS/OIS); Fletcher, John A. (CMS/OIS); Van, Hung B. (CMS/OIS); Grothe, Kirk A. (CMS/OIS); Lyles, Darrin V. (CMS/OIS); 'Venky Natarajan' (vnatarajan@gssinc.com) (vnatarajan@gssinc.com); lynn.goodrich@cgifederal.com; Thomas.Kirk@gss-cgi.com; 'Ramamoorthy, Balaji Manikandan (CGI Federal)' (balajimanikandan.ramamoorthy@cgifederal.com); Outerbridge, Monique (CMS/OIS)

**Subject:** Security Items that Need Attention

QSSI and CGI,

I am writing to highlight several security incidents that need your attention. As they are security issues, please consider the Remedy ticket your authorization to act. I am only sending the Remedy numbers to avoid transmitting too much detail. By tomorrow, please communicate back to use their status (closed, in process, etc) and at least a tentative date for resolution.

1. These are the two that Tom Schankweiler raised today.
  - INC000002589982
  - artf161265 INC2598675
2. Additionally, we identified several open tickets in Remedy.
  - 2614246
  - 2614253
  - 2614255
  - 2614297
  - 2614299
  - 2614303
  - 2614304
  - 2614305
  - 2614307
  - 2614309
  - 2614310
  - 2614311
  - 2614313
  - 2614316
  - 2614317
  - 2614318
  - 2614319
  - 2614320
  - 2614321
  - 2614322
  - 2614323
  - 2614324
  - 2614325
  - 2614326
  - 2614328
  - 2614329
  - 2614330
  - 2614331
  - 2614332
  - 2614327
  - 2614333
  - 2614334
  - 2614335
  - 2614336
  - 2614337
  - 2614338
  - 2614339
  - 2614340

• 2614341

2

**Todd Coutts**

Centers for Medicare & Medicaid Services

Office of Information Services

301-492-5139 (office) (b)(6) (mobile) | [todd.coutts1@cms.hhs.gov](mailto:todd.coutts1@cms.hhs.gov)

7700 Wisconsin Ave Bethesda MD 20814 | Location: 9308

**From:** Schankweiler, Thomas W. (CMS/OIS)

**Sent:** Tuesday, November 26, 2013 12:41 PM

**To:** Coutts, Todd (CMS/OIS); Kane, David (CMS/OIS); Michael Finkel

**Cc:** Warren, Kevin (CMS/OIS); Fletcher, John A. (CMS/OIS); Van, Hung B. (CMS/OIS); Grothe, Kirk A. (CMS/OIS); Lyles, Darrin V. (CMS/OIS)

**Subject:** INC000002589982 Need details regarding

NotResp

Todd,

I would like to escalate this ticket NC000002589982 as being high risk on the defect list. I know that a bunch of security risk have recently appeared on the list but I wanted to let you know this one is considered high priority. In total we now have two tickets that are considered high priority. Contact me if you have any questions.

Thanks,

Tom

**From:** Ramamoorthy, Balaji Manikandan (CGI Federal) [<mailto:balajimanikandan.ramamoorthy@cgifederal.com>]

**Sent:** Tuesday, November 26, 2013 10:52 AM

**To:** Schankweiler, Thomas W. (CMS/OIS); Willard, Adam (CMS/CTR)

**Cc:** Warren, Kevin (CMS/OIS); Quaintance, Eric (CGI Federal); Dhas, Navin (CGI Federal); Alford, Justin (CGI Federal); Martin, Rich (CGI Federal)

**Subject:** RE: artf160711 / INC000002589982 Need details regarding

NotResp

Hi Tom,

We promoted the code fix into production. Apparently the security enforcement is turned off.

The Alfresco documents (notices) that are saved are not having the proper meta data populated to turn on the enforcements. So in addition to the fix that has been rolled in the following actions needs to occur.

1. Do a manual batch job to update the meta data for all the existing notices.
2. Have the developers fix the code so that any new notices that are saved has the proper metadata for enforcement.

These 2 action items are being coordinated internally right now. We don't have an ETA yet.

Thanks

Balaji M. Ramamoorthy

**From:** Schankweiler, Thomas W. (CMS/OIS) [<mailto:thomas.schankweiler@cms.hhs.gov>]

**Sent:** Tuesday, November 26, 2013 10:42 AM

**To:** Ramamoorthy, Balaji Manikandan (CGI Federal); Willard, Adam (CMS/CTR)  
**Cc:** Warren, Kevin (CMS/OIS); Quaintance, Eric (CGI Federal); Dhas, Navin (CGI Federal)  
**Subject:** artf160711 / INC000002589982 Need details regarding [NotResp]

Balaji, Adam, and Kevin

I am looking for an update on this ticket. Can someone provide be a status of where we are with this item? Has it been corrected? Is the situation still occurring?

Thanks,

Tom

**From:** Ramamoorthy, Balaji Manikandan (CGI Federal) [mailto:balajimanikandan.ramamoorthy@cgifederal.com]  
**Sent:** Wednesday, November 06, 2013 12:39 PM  
**To:** Willard, Adam (CMS/CTR)  
**Cc:** Warren, Kevin (CMS/OIS); Schankweiler, Thomas W. (CMS/OIS); Quaintance, Eric (CGI Federal); Dhas, Navin (CGI Federal)  
**Subject:** RE: Need details regarding [NotResp]

Hi Adam,

There are multiple instances of Alfresco. We expect [NotResp] guarantees for the uniqueness across JVM's. We did go this route to see if there were duplicates.

So far the root cause has not been determined for the notices. In this particular instance we did see that the username were closely identical between the user1 and user2. There was a special character "-" at the end (and that was the only difference). We are also looking into the [NotResp] query to see how it behaves and whether it has to be tweaked.

Thanks

Balaji M. Ramamoorthy

**From:** Willard, Adam (CMS/CTR) [mailto:Adam.Willard@cms.hhs.gov]  
**Sent:** Wednesday, November 06, 2013 12:05 PM  
**To:** Ramamoorthy, Balaji Manikandan (CGI Federal)  
**Cc:** Warren, Kevin (CMS/OIS); Schankweiler, Thomas W. (CMS/OIS); Quaintance, Eric (CGI Federal); Dhas, Navin (CGI Federal)  
**Subject:** RE: Need details regarding [NotResp]

Is Alfresco just 1 instance or are there several instances in production? If there are multiple systems generating a [NotResp] there could be collisions.

What was the analysis from the Users who said they saw someone's Notice instead of theirs. Was there any check to see if the [NotResp] or that user and the other user was the same?

**Adam Willard** (Contractor)  
703-354-2229 x513 (Direct)  
(b)(6) (Mobile)  
Adam.Willard@cms.hhs.gov

[NotResp]  
CMS Security Team



Consumer Information & Insurance Systems Group (CIISG)

Centers for Medicare & Medicaid Services (CMS)

703-594-4961/

NotResp

ciisg-soc@cms.hhs.gov

---

**From:** Ramamoorthy, Balaji Manikandan (CGI Federal) [balajimanikandan.ramamoorthy@cgifederal.com]

**Sent:** Wednesday, November 06, 2013 11:47 AM

**To:** Willard, Adam (CMS/CTR)

**Cc:** Warren, Kevin (CMS/OIS); Schankweiler, Thomas W. (CMS/OIS); Quaintance, Eric (CGI Federal); Dhas, Navin (CGI Federal)

**Subject:** RE: Need details regarding

NotResp

Hi Adam,

The eligibility notices are stored in **NotResp** and the URI's for the notices are stored against the user record in Marklogic.

The **NotResp** or the PDF document itself is generated by **NotResp** and it is sufficiently random.

We did identify this issue internally and it is in the list of high priority items to be fixed. I will track down on the ETA for the fix and let you know.

I agree that in the meantime to see if the rate control can be applied to this specific URL.

Thanks

Balaji M. Ramamoorthy

**From:** Willard, Adam (CMS/CTR) [mailto:Adam.Willard@cms.hhs.gov]

**Sent:** Wednesday, November 06, 2013 9:37 AM

**To:** Ramamoorthy, Balaji Manikandan (CGI Federal)

**Cc:** Warren, Kevin (CMS/OIS); Schankweiler, Thomas W. (CMS/OIS); Quaintance, Eric (CGI Federal)

**Subject:** Need details regarding

NotResp

**Importance:** High

Balaji,

I noticed this morning that it is possible for anyone to run a brute force against healthcare.gov to obtain the results of their eligibility.

I need to know where you are grabbing the file from **NotResp** something else). Is that system publicly accessible?

We need to know if there is anyway to put in permission checking of the workspace url **NotResp** against the list of possible **NotResp** for a user.

I sent Shima (an **NotResp** security Analyst) my eligibility URL and she was able to see my results in PDF format.

We are looking into a Rate Control for the **NotResp** to block or limit access to this screen if several attempts are made over X period of time.

**Adam Willard** (Contractor)

703-354-2229 x513 (Direct)

(b)(6)

(Mobile)

Adam.Willard@cms.hhs.gov

CMS **NotResp** Security Team

Consumer Information & Insurance Systems Group (CIISG)

Centers for Medicare & Medicaid Services (CMS)

703-594-4961/ (b)(6)

ciisg-soc@cms.hhs.gov

Message

**From:** Schankweiler, Thomas W. (CMS/OIS) [redacted] NotResp  
[redacted] NotResp  
on behalf of Schankweiler, Thomas W. (CMS/OIS)  
**Sent:** 12/3/2013 3:31:33 PM  
**To:** 'Hank Youd' [hyoud@foregroundsecurity.com]; Warren, Kevin (CMS/OIS) [redacted] NotResp  
[redacted] NotResp Howard, Jacqueline Y. (CMS/OIS) [redacted] NotResp  
[redacted] NotResp  
**Subject:** RE: Security Items that Need Attention

Kevin,

Lets be sure to give Jacqueline a complete list of who needs their access updated so that they can view the IM page. I assume you have that list.

Tom

**From:** Hank Youd [mailto:hyoud@foregroundsecurity.com]  
**Sent:** Tuesday, December 03, 2013 10:27 AM  
**To:** Schankweiler, Thomas W. (CMS/OIS); Warren, Kevin (CMS/OIS); Howard, Jacqueline Y. (CMS/OIS)  
**Subject:** Re: Security Items that Need Attention

I can get there, but both sections are completely empty.

Thanks,  
Hank

**From:** <Schankweiler>, "Thomas W. (CMS/OIS)" <thomas.schankweiler@cms.hhs.gov>  
**Date:** Tuesday, December 3, 2013 10:23 AM  
**To:** "Warren, Kevin (CMS/OIS)" <Kevin.Warren@cms.hhs.gov>, "Howard, Jacqueline Y. (CMS/OIS)" <Jacqueline.Howard@cms.hhs.gov>  
**Cc:** Hank Youd <hyoud@foregroundsecurity.com>  
**Subject:** RE: Security Items that Need Attention

Hank,

Try this. Click on Consoles, then Incident Management

BMC **NotResp** SERVICE MANAGEMENT

Welcome, THOMAS W. SCHANKWEILER

Close Help

Overview Console

Company: [Dropdown] View By: All My Groups

Console List

Create View Print Search For Ticket

Showing 1 - 20 of 20 Page: 1

Request ID	Parent Request	Request Type	Status	Priority	Assignee	Assigned
INC00000253000		Incident	Assigned	Medium	vSOC	KEVIN WARR
INC000002583050		Incident	Assigned	Medium	vSOC	LESLIE A REI
INC000002583827		Incident	Pending	Medium	vSOC	KEVIN WARR
INC000002589982		Incident	Pending	Medium	vSOC	KEVIN WARR
INC000002591251		Incident	Progress	Medium	vSOC	KEVIN WARR
INC000002595237		Incident	Assigned	Medium	vSOC	
INC000002618890		Incident	Progress	Medium	vSOC	George Grayst
INC000002618965		Incident	Progress	Medium	vSOC	George Grayst
INC000002618986		Incident	Progress	Medium	vSOC	George Grayst
INC000002620017		Incident	Progress	Medium	vSOC	George Grayst
INC000002620036		Incident	Progress	Medium	vSOC	George Grayst
INC000002620064		Incident	Progress	Medium	vSOC	George Grayst
INC000002620102		Incident	Progress	Medium	vSOC	George Grayst
INC000002620118		Incident	Progress	Medium	vSOC	George Grayst
INC000002620133		Incident	Progress	Medium	vSOC	George Grayst
INC000002620145		Incident	Progress	Medium	vSOC	George Grayst
INC000002620153		Incident	Progress	Medium	vSOC	George Grayst
INC000002620163		Incident	Progress	Medium	vSOC	George Grayst
INC000002620187		Incident	Progress	Medium	vSOC	George Grayst
INC000002620178		Incident	Progress	Medium	vSOC	George Grayst

NotResp

That should give you this screen where you can see all the items in the queue.

BMC **NotResp** SERVICE MANAGEMENT - Incident Management

Welcome, THOMAS W. SCHANKWEILER

Close Help

Incident Console

Company: [Dropdown] View By: All My Groups

Incidents

Create View Print Quick Actions Add To Watch

Showing 1 - 50 of 63 Page: 1

ID	Priority	Status	Assignee	Target D.	SLA Status
INC00000259	Medium	Assigned	KEVIN WARREN		
INC000002569	Medium	Assigned			
INC000002583	Medium	Assigned	LESLIE A REINHOLD		
INC000002587	Medium	Pending	KEVIN WARREN		
INC000002589	Medium	Pending	KEVIN WARREN		
INC000002597	Medium	In Progress	KEVIN WARREN		
INC000002599	Medium	Assigned			
INC000002614	Medium	In Progress	Reed Erickson		
INC000002615	Medium	In Progress	David Erickson		

Incident Detail and Fields

Status Reason: Monitoring Incident

Assigned Group: vSOC

Reported Date: 10/6/2013 9:53:09 AM

Customer: CSIRT, CSIRT

Notes: From Orlando Mark (CMS/CTR)  
Sent: Sunday, October

Service:

Create View Report Show Ticket

Showing 1 - 2 of 2 Page: 1

Summary	Submit Date
General Information	10/6/2013 11:30:03 AM
General Information	10/6/2013 10:33:13 AM

NotResp

**From:** Warren, Kevin (CMS/OIS)  
**Sent:** Tuesday, December 03, 2013 9:40 AM  
**To:** Howard, Jacqueline Y. (CMS/OIS)  
**Cc:** Schankweiler, Thomas W. (CMS/OIS); Hank Youd ([hyoud@foregroundsecurity.com](mailto:hyouud@foregroundsecurity.com))  
**Subject:** Security Items that Need Attention

Jacqueline,

Some of our team members are still experiencing problems with NotResp and access to our security queue. All the members of Marketplace Security Team require read/write access. Let me know if you need any information from me.

Thanks in advance.

Kevin Warren | Centers for Medicare and Medicaid Services (CMS) | Office of Information Services (OIS) | Consumer Information and Insurance Systems Group (CIISG) | 7700 Wisconsin Ave (9380-A) | Bethesda, Maryland | 301.492.4381 (O)

**From:** Youd, Hank (CMS/CTR)  
**Sent:** Tuesday, December 03, 2013 9:23 AM  
**To:** Schankweiler, Thomas W. (CMS/OIS); Warren, Kevin (CMS/OIS)  
**Cc:** Villar, Manuel (CMS/CTR)  
**Subject:** RE: Security Items that Need Attention

UPDATE,

Correction, we can get to a search page to search ticket numbers but the Incident Management page is empty. Very odd that in order to see anything, it has to be manually search on.

Thanks,  
Hank

**From:** Youd, Hank (CMS/CTR)  
**Sent:** Tuesday, December 03, 2013 9:14 AM  
**To:** Schankweiler, Thomas W. (CMS/OIS); Warren, Kevin (CMS/OIS)  
**Cc:** Villar, Manuel (CMS/CTR)  
**Subject:** RE: Security Items that Need Attention

Tom,  
We are still having remedy issues, I finally got in but I can only see tickets that are related to my CMS account. I don't see any queues that are IR related. Boden sees the same thing so there must be some permissions that need to be granted so we can see the correct queues.

Thanks,  
Hank

**From:** Schankweiler, Thomas W. (CMS/OIS)  
**Sent:** Tuesday, December 03, 2013 8:52 AM  
**To:** Youd, Hank (CMS/CTR); Warren, Kevin (CMS/OIS)  
**Cc:** Villar, Manuel (CMS/CTR)  
**Subject:** FW: Security Items that Need Attention

Kevin and Hank,

We need to work on this in the afternoon.

Kevin you setup a meeting from noon-1pm please.

Hank, in preparation for the meeting I need a report (spreadsheet or something) of what these incidents are and if they are currently open or closed.

NotResp

Thanks,

Tom

**From:** Coutts, Todd (CMS/OIS)  
**Sent:** Tuesday, November 26, 2013 3:48 PM  
**To:** Schankweiler, Thomas W. (CMS/OIS); Kane, David (CMS/OIS); Michael Finkel  
**Cc:** Warren, Kevin (CMS/OIS); Fletcher, John A. (CMS/OIS); Van, Hung B. (CMS/OIS); Grothe, Kirk A. (CMS/OIS); Lyles, Darrin V. (CMS/OIS); 'Venky Natarajan' (vnatarajan@qssinc.com) (vnatarajan@qssinc.com); lynn.goodrich@cgifederal.com; Thomas.Kirk@gss-cgi.com; 'Ramamoorthy, Balaji Manikandan (CGI Federal)' (balajimanikandan.ramamoorthy@cgifederal.com); Outerbridge, Monique (CMS/OIS)  
**Subject:** Security Items that Need Attention

QSSI and CGI,

I am writing to highlight several security incidents that need your attention. As they are security issues, please consider the Remedy ticket your authorization to act. I am only sending the Remedy numbers to avoid transmitting too much detail. By tomorrow, please communicate back to use their status (closed, in process, etc) and at least a tentative date for resolution.

1. These are the two that Tom Schankweiler raised today.
  - INC000002589982
  - artf161265 INC2598675
2. Additionally, we identified several open tickets in Remedy.
  - 2614246
  - 2614253
  - 2614255
  - 2614297
  - 2614299
  - 2614303
  - 2614304
  - 2614305
  - 2614307
  - 2614309

- . 2614310
- . 2614311
- . 2614313
- . 2614316
- . 2614317
- . 2614318
- . 2614319
- . 2614320
- . 2614321
- . 2614322
- . 2614323
- . 2614324
- . 2614325
- . 2614326
- . 2614328
- . 2614329
- . 2614330
- . 2614331
- . 2614332
- . 2614327
- . 2614333
- . 2614334
- . 2614335
- . 2614336
- . 2614337
- . 2614338
- . 2614339
- . 2614340
- . 2614341

**Todd Coutts**

Centers for Medicare & Medicaid Services  
Office of Information Services

301-492-5139 (office) | (b)(6) | mobile) | [todd.coutts1@cms.hhs.gov](mailto:todd.coutts1@cms.hhs.gov)  
7700 Wisconsin Ave Bethesda MD 20814 | Location: 9308

**From:** Schankweiler, Thomas W. (CMS/OIS)

**Sent:** Tuesday, November 26, 2013 12:41 PM

**To:** Coutts, Todd (CMS/OIS); Kane, David (CMS/OIS); Michael Finkel

**Cc:** Warren, Kevin (CMS/OIS); Fletcher, John A. (CMS/OIS); Van, Hung B. (CMS/OIS); Grothe, Kirk A. (CMS/OIS); Lyles, Darrin V. (CMS/OIS)

**Subject:** INC000002589982 Need details regarding [NotResp]

Todd,

I would like to escalate this ticket NC000002589982 as being high risk on the defect list. I know that a bunch of security risk have recently appeared on the list but I wanted to let you know this one is considered high priority. In total we now have two tickets that are considered high priority. Contact me if you have any questions.

Thanks,

Tom



**From:** Ramamoorthy, Balaji Manikandan (CGI Federal) [mailto:balajimanikandan.ramamoorthy@cgifederal.com]

**Sent:** Tuesday, November 26, 2013 10:52 AM

**To:** Schankweiler, Thomas W. (CMS/OIS); Willard, Adam (CMS/CTR)

**Cc:** Warren, Kevin (CMS/OIS); Quaintance, Eric (CGI Federal); Dhas, Navin (CGI Federal); Alford, Justin (CGI Federal); Martin, Rich (CGI Federal)

**Subject:** RE: artf160711 / INC000002589982 Need details regarding [NotResp]

Hi Tom,

We promoted the code fix into production. Apparently the security enforcement is turned off.

The [NotResp] documents (notices) that are saved are not having the proper meta data populated to turn on the enforcements. So in addition to the fix that has been rolled in the following actions needs to occur.

1. Do a manual batch job to update the meta data for all the existing notices.
2. Have the developers fix the code so that any new notices that are saved has the proper metadata for enforcement.

These 2 action items are being coordinated internally right now. We don't have an ETA yet.

Thanks

Balaji M. Ramamoorthy

**From:** Schankweiler, Thomas W. (CMS/OIS) [mailto:thomas.schankweiler@cms.hhs.gov]

**Sent:** Tuesday, November 26, 2013 10:42 AM

**To:** Ramamoorthy, Balaji Manikandan (CGI Federal); Willard, Adam (CMS/CTR)

**Cc:** Warren, Kevin (CMS/OIS); Quaintance, Eric (CGI Federal); Dhas, Navin (CGI Federal)

**Subject:** artf160711 / INC000002589982 Need details regarding [b)(5)]

Balaji, Adam, and Kevin

I am looking for an update on this ticket. Can someone provide be a status of where we are with this item? Has it been corrected? Is the situation still occurring?

Thanks,

Tom

**From:** Ramamoorthy, Balaji Manikandan (CGI Federal) [mailto:balajimanikandan.ramamoorthy@cgifederal.com]

**Sent:** Wednesday, November 06, 2013 12:39 PM

**To:** Willard, Adam (CMS/CTR)

**Cc:** Warren, Kevin (CMS/OIS); Schankweiler, Thomas W. (CMS/OIS); Quaintance, Eric (CGI Federal); Dhas, Navin (CGI Federal)

**Subject:** RE: Need details regarding DocumentFromECM?fileIdentifier=

Hi Adam,

There are multiple instances of [NotResp]. We expect [NotResp] guarantees for the uniqueness across JVM's. We did go this route to see if there were duplicates.



So far the root cause has not been determined for the notices. In this particular instance we did see that the username were closely identical between the user1 and user2. There was a special character "-" at the end (and that was the only difference). We are also looking into the [NotResp] query to see how it behaves and whether it has to be tweaked.

Thanks

Balaji M. Ramamoorthy

**From:** Willard, Adam (CMS/CTR) [mailto:Adam.Willard@cms.hhs.gov]

**Sent:** Wednesday, November 06, 2013 12:05 PM

**To:** Ramamoorthy, Balaji Manikandan (CGI Federal)

**Cc:** Warren, Kevin (CMS/OIS); Schankweiler, Thomas W. (CMS/OIS); Quaintance, Eric (CGI Federal); Dhas, Navin (CGI Federal)

**Subject:** RE: Need details regarding [redacted] (b)(5)

Is Alfresco just 1 instance or are there several instances in production? If there are multiple systems generating a GUID there could be collisions.

What was the analysis from the Users who said they saw someone's Notice instead of theirs. Was there any check to see if the GUID for that user and the other user was the same?

**Adam Willard** (Contractor)

703-354-2229 x513 (Direct)

[redacted] (b)(6) Mobile)

Adam.Willard@cms.hhs.gov

**CMS [Not Re] Security Team**

Consumer Information & Insurance Systems Group (CIISG)

Centers for Medicare & Medicaid Services (CMS)

703-594-4961 [redacted] (b)(6)

ciisg-soc@cms.hhs.gov

---

**From:** Ramamoorthy, Balaji Manikandan (CGI Federal) [balajimanikandan.ramamoorthy@cgifederal.com]

**Sent:** Wednesday, November 06, 2013 11:47 AM

**To:** Willard, Adam (CMS/CTR)

**Cc:** Warren, Kevin (CMS/OIS); Schankweiler, Thomas W. (CMS/OIS); Quaintance, Eric (CGI Federal); Dhas, Navin (CGI Federal)

**Subject:** RE: Need details regarding [redacted] (b)(5)

Hi Adam,

The eligibility notices are stored in [NotResp] and the URI's for the notices are stored against the user record in Marklogic.

The GUID for the PDF document itself is generated by [NotResp] and it is sufficiently random.

We did identify this issue internally and it is in the list of high priority items to be fixed. I will track down on the ETA for the fix and let you know.

I agree that in the meantime to see if the rate control can be applied to this specific URL.

Thanks

Balaji M. Ramamoorthy

**From:** Willard, Adam (CMS/CTR) [mailto:Adam.Willard@cms.hhs.gov]

**Sent:** Wednesday, November 06, 2013 9:37 AM

**To:** Ramamoorthy, Balaji Manikandan (CGI Federal)

**Cc:** Warren, Kevin (CMS/OIS); Schankweiler, Thomas W. (CMS/OIS); Quaintance, Eric (CGI Federal)

**Subject:** Need details regarding (b)(5)

**Importance:** High

Balaji,

I noticed this morning that it is possible for anyone to run a brute force against healthcare.gov to obtain the results of their eligibility.

I need to know where you are grabbing the file from NotResp or something else). Is that system publicly accessible?

We need to know if there is anyway to put in permission checking of the workspace url GUID against the list of possible GUIDs for a user.

I sent Shima (an XOC Security Analyst) my eligibility URL and she was able to see my results in PDF format.

We are looking into a Rate Control for the Akamai WAF to block or limit access to this screen if several attempts are made over X period of time.

**Adam Willard** (Contractor)

703-354-2229 x513 (Direct)

(b)(6) (Mobile)

Adam.Willard@cms.hhs.gov

**CMS Security Team**

Consumer Information & Insurance Systems Group (CIISG)

Centers for Medicare & Medicaid Services (CMS)

703-594-4961 (b)(6)

ciisg-soc@cms.hhs.gov

Message

**From:** Schankweiler, Thomas W. (CMS/OIS) [NotResp]  
 on behalf of [NotResp]  
**Sent:** 12/3/2013 4:48:55 PM  
**To:** Reinhold, Leslie A. (CMS/OEM) [NotResp]  
**Subject:** FW: Data.Healthcare.gov.

**From:** Joe Pringle [mailto:joe.pringle@socrata.com]  
**Sent:** Wednesday, November 20, 2013 6:08 AM  
**To:** Willard, Adam (CMS/CTR)  
**Cc:** Patel, Ketan (CMS/OC); Orlando, Mark (CMS/CTR); Booth, Jon G. (CMS/OC); Hiko Naito; Matthew Vanden Boogart; Slavinsky, Gary F. (CMS/OC); [NotResp] Schankweiler, Thomas W. (CMS/OIS)  
**Subject:** Re: Data.Healthcare.gov.

We've been looking at things and one thing our Ops team wanted to **recommend is for quick action is for healthcare.gov to take down the reverse proxy to data.healthcare.gov**. We were not aware this is in place and unfortunately do not have control over it. We'll also follow up on the request to block the console to reduce the burden on responding to non-issues. I'm still working with our product team to determine whether that is a necessary feature for some customers.

Joe

**Socrata**

o: 202-747-0024  
 m: [NotResp]  
[joe.pringle@socrata.com](mailto:joe.pringle@socrata.com)

On Tue, Nov 19, 2013 at 8:47 PM, Willard, Adam (CMS/CTR) <[Adam.Willard@cms.hhs.gov](mailto:Adam.Willard@cms.hhs.gov)> wrote:  
 Joe, thank you for your response. Basically we understand the functionality of this screen. However, if "security researchers" are submitting things like this as vulnerabilities. If this does not need to exist or if we can block via a WAF, it reduces the future burden of having to respond to non issues.

Our stance on this functionality is that if it isn't critical to operation of the system, the smallest footprint deployed to the server reduces the attack surface.

I am available tonight if needed.

**Adam Willard** (Contractor)  
 703-354-2229 x513 (Direct)  
 [NotResp] (Mobile)  
[Adam.Willard@cms.hhs.gov](mailto:Adam.Willard@cms.hhs.gov)

**CMS Res. Security Team**  
 Consumer Information & Insurance Systems Group (CIISG)  
 Centers for Medicare & Medicaid Services (CMS)  
 703-594-4961 [NotResp]  
[ciisg-soc@cms.hhs.gov](mailto:ciisg-soc@cms.hhs.gov)

---

**From:** Patel, Ketan (CMS/OC)  
**Sent:** Tuesday, November 19, 2013 8:31 PM  
**To:** Joe Pringle; Willard, Adam (CMS/CTR); Orlando, Mark (CMS/CTR)  
**Cc:** Booth, Jon G. (CMS/OC); Hiko Naito; Matthew Vanden Boogart; Slavinsky, Gary F. (CMS/OC); NotResp  
NotResp Schankweiler, Thomas W. (CMS/OIS)  
**Subject:** RE: [Data.Healthcare.gov](#).

Joe,

I have copied Adam & Mark who represent CMS security team to this email.

Thanks,

Ketan

**From:** Joe Pringle [mailto:[joe.pringle@socrata.com](mailto:joe.pringle@socrata.com)]  
**Sent:** Tuesday, November 19, 2013 6:24 PM  
**To:** Patel, Ketan (CMS/OC)  
**Cc:** Booth, Jon G. (CMS/OC); Hiko Naito; Matthew Vanden Boogart; Slavinsky, Gary F. (CMS/OC); NotResp  
**Subject:** Re: [Data.Healthcare.gov](#).

Hi Ketan -

Any chance we could have a conversation about this with the right people on the CMS side? We don't view this to be a security risk as we're simply replicating the NotResp functionality.

That said, I want to make sure we're understanding the full picture and maybe having quick call on this would help us better understand the concern and come up with a good solution.

If Daniel or others are available this evening I could assemble the right people on the Socrata side. Alternatively I'll be there in person tomorrow AM and we could talk about it then.

Let me know what works best.

Joe

**Socrata**

o: 202-747-0024

m (b)(6)  
joe.pringle@socrata.com

On Tue, Nov 19, 2013 at 3:47 PM, Patel, Ketan (CMS/OC) <Ketan.Patel@cms.hhs.gov> wrote:

Joe,

Our security team would like to block **data.healthcare.gov/console** since it allows a user to type arbitrary data into the screen. Please let us know the impact of doing this and how quickly we can do this.

NotResp

Thanks,

Ketan Patel

**From:** Joe Pringle <joe.pringle@socrata.com>

**Date:** Tuesday, November 19, 2013 at 3:17 PM

**To:** Ketan PATEL <ketan.patel@cms.hhs.gov>

**Cc:** Jon Booth BB <Jon.Booth@cms.hhs.gov>, Hiko Naito <hiko.naito@socrata.com>, Matthew Boogart <matthew.vandenboogart@socrata.com>, "Slavinsky, Gary F. (CMS/OC)" <Gary.Slavinsky@cms.hhs.gov>

**Subject:** Re: Data.Healthcare.gov.

Hi Ketan -

Here's our assessment of the items related to Socrata in the report you sent.

### 3.4) Test Domains Exposed on the Internet

The only datasets that were indexed by search engines were public datasets. Some were test datasets but but the datasets have since been removed and data is no longer available, even if you try to view cached version.

### 3.5) Exposed Profiles

- This is our public user profile search API and publicly viewable profile information which doesn't reveal any private user information that could be exploited in any way.

- There is no connection or integration between Socrata platform user accounts and healthcare.gov user accounts. They are completely separate.

I'm available to discuss and we can also provide this response in a more formal way as needed. Let me know what any next steps on this would be helpful.

Joe

#### Socrata

o: 202-747-0024

m: (b)(6)  
joe.pringle@socrata.com

----- Forwarded message -----

From: **Patel, Ketan (CMS/OC)** <Ketan.Patel@cms.hhs.gov>

Date: Tue, Nov 19, 2013 at 1:09 PM

Subject: Re: Data.Healthcare.gov.

To: Joe Pringle <joe.pringle@socrata.com>, "Booth, Jon G. (CMS/OC)" <Jon.Booth@cms.hhs.gov>

Cc: Hiko Naito <hiko.naito@socrata.com>, Matthew Vanden Boogart <matthew.vandenboogart@socrata.com>, "Slavinsky, Gary F. (CMS/OC)" <Gary.Slavinsky@cms.hhs.gov>

Joe,

Can you check at below report and related Socrata specific findings can you provide us mitigation plan immediate actions taken informal document. This biased on security hearing at the hill today. This is time sensitive activity.

<http://science.house.gov/sites/republicans.science.house.gov/files/documents/HHRG-113-SY-WState-DKennedy-20131119.pdf>

Reply back to all.

Thanks,

Ketan Patel

**From:** Joe Pringle <[joe.pringle@socrata.com](mailto:joe.pringle@socrata.com)>

**Date:** Tuesday, November 19, 2013 at 9:35 AM

**To:** Jon Booth BB <[Jon.Booth@cms.hhs.gov](mailto:Jon.Booth@cms.hhs.gov)>

**Cc:** Ketan PATEL <[ketan.patel@cms.hhs.gov](mailto:ketan.patel@cms.hhs.gov)>, Hiko Naito <[hiko.naito@socrata.com](mailto:hiko.naito@socrata.com)>, Matthew Boogart <[matthew.vandenboogart@socrata.com](mailto:matthew.vandenboogart@socrata.com)>, "Slavinsky, Gary F. (CMS/OC)" <[Gary.Slavinsky@cms.hhs.gov](mailto:Gary.Slavinsky@cms.hhs.gov)>

**Subject:** Re: [Data.Healthcare.gov](http://Data.Healthcare.gov).

Hi Jon

Here's an update on this (actually nothing has really changed from last night but I just wanted to resend what I provided last night in the form of talking points). Please don't hesitate to call me on my cell: (b)(6) if any of you have questions or want to discuss further.

1) Based on the information we have been given, we think it's likely this is referring to our public user profile search API which doesn't reveal any private user information that could be exploited.

2) There is no connection or integration between Socrata platform user accounts and [healthcare.gov](http://healthcare.gov) user accounts. They are completely separate.

3) Because of this we don't think the vulnerability characterized in your original email is a valid concern.

4) We have been monitoring and there are no indications of any malicious activity targeting the Socrata platform or [data.healthcare.gov](http://data.healthcare.gov).

We are still standing by to investigate this further if / when you have any additional info.

Joe

**Socrata**

o: [202-747-0024](tel:202-747-0024)

m: (b)(6)  
[joe.pringle@socrata.com](mailto:joe.pringle@socrata.com)

On Mon, Nov 18, 2013 at 7:07 PM, Booth, Jon G. (CMS/OC) <[Jon.Booth@cms.hhs.gov](mailto:Jon.Booth@cms.hhs.gov)> wrote:

We don't have any additional details but our office of legislation has agreed to pass on any information they get.

We independently were thinking the exact same thing you were - profile search. If so, that's not a vulnerability.

On Nov 18, 2013, at 7:04 PM, "Joe Pringle" <[joe.pringle@socrata.com](mailto:joe.pringle@socrata.com)> wrote:

Our team is looking at this now. Is there any more detail you can provide or point us to someone on your side that our Ops team could get more info from? If someone there has it, we'd like to see an example of the exploit. One possibility is that this is simply our public user search API which doesn't reveal any credentials or email addresses (only publicly available user profile information).

**Socrata**

o: [202-747-0024](tel:202-747-0024)



m. (b)(6)  
joe.pringle@socrata.com

On Mon, Nov 18, 2013 at 6:32 PM, Booth, Jon G. (CMS/OC) <[Jon.Booth@cms.hhs.gov](mailto:Jon.Booth@cms.hhs.gov)> wrote:

Joe,

This is not public yet, but the security vulnerability below was submitted to CMS today. Supposedly this will be included as part of a congressional hearing tomorrow. Can you investigate this further based on the description below? We don't necessarily believe the claims below, but we want to investigate to insure there is not an issue.

Thanks,

Jon

—

The website [data.healthcare.gov](http://data.healthcare.gov) suffers from a **NotResp** attack which can extract all users contained on the site. Since [data.healthcare.gov](http://data.healthcare.gov) is integrated into the [healthcare.gov](http://healthcare.gov) site, this may expose a much larger problem with all users on the site. With the attack, an individual can extract all users, email addresses, unique ID's, and personal information related to the individual. The information obtained from the site can further be used to launch attacks against individuals that have registered for the website. This vulnerability is due to the inability to restrict permissions on the website and allow anyone on the public Internet to enumerate any information about individuals that have registered for the [data.healthcare.gov](http://data.healthcare.gov) website.

**From:** Joe Pringle <[joe.pringle@socrata.com](mailto:joe.pringle@socrata.com)>

**Date:** Monday, November 18, 2013 at 5:18 PM

**To:** Ketan Patel BB <[Ketan.Patel@cms.hhs.gov](mailto:Ketan.Patel@cms.hhs.gov)>

**Cc:** Hiko Naito <[hiko.naito@socrata.com](mailto:hiko.naito@socrata.com)>, Matthew Vanden Boogart <[matthew.vandenboogart@socrata.com](mailto:matthew.vandenboogart@socrata.com)>, "Slavinsky, Gary F. (CMS/OC)" <[Gary.Slavinsky@cms.hhs.gov](mailto:Gary.Slavinsky@cms.hhs.gov)>, Jon Booth <[jon.booth@cms.hhs.gov](mailto:jon.booth@cms.hhs.gov)>

**Subject:** Re: [Data.Healthcare.gov](http://Data.Healthcare.gov).

Our ops team is looking at it now. Is there a specific time period we should be looking at? Just today?

Joe

**Socrata**

o: 202-747-0024

m [REDACTED] (b)(6)  
joe.pringle@socrata.com

On Mon, Nov 18, 2013 at 5:12 PM, Patel, Ketan (CMS/OC) <Ketan.Patel@cms.hhs.gov> wrote:

Can we check into recent logs and see if anything has been attempted.

Thanks

Ketan

**From:** Joe Pringle <joe.pringle@socrata.com>

**Date:** Monday, November 18, 2013 at 5:10 PM

**To:** Ketan PATEL <ketan.patel@cms.hhs.gov>

**Cc:** Hiko Naito <hiko.naito@socrata.com>, Matthew Boogart <matthew.vandenboogart@socrata.com>, "Slavinsky, Gary F. (CMS/OC)" <Gary.Slavinsky@cms.hhs.gov>, Jon Booth BB <Jon.Booth@cms.hhs.gov>

**Subject:** Re: Data.Healthcare.gov.

I'm alerting our security and operations folks here to be on the lookout for anything that looks abnormal (and report anything they've already detected). Our ops team has tools in place to detect malicious activity.

**Socrata**

o: 202-747-0024

m [REDACTED] (b)(6)  
joe.pringle@socrata.com

On Mon, Nov 18, 2013 at 4:59 PM, Patel, Ketan (CMS/OC) <[Ketan.Patel@cms.hhs.gov](mailto:Ketan.Patel@cms.hhs.gov)> wrote:

Thanks. We need to know if any socrata user accounts are being exploited or is [data.healthcare.gov](http://data.healthcare.gov) being targeting for hack? Doe stour security team get notified when any service attacks are made.

Thanks

Ketan

**From:** Joe Pringle <[joe.pringle@socrata.com](mailto:joe.pringle@socrata.com)>

**Date:** Monday, November 18, 2013 at 4:51 PM

**To:** Ketan PATEL <[ketan.patel@cms.hhs.gov](mailto:ketan.patel@cms.hhs.gov)>, Hiko Naito <[hiko.naito@socrata.com](mailto:hiko.naito@socrata.com)>, Matthew Boogart <[matthew.vandenboogart@socrata.com](mailto:matthew.vandenboogart@socrata.com)>

**Cc:** "Slavinsky, Gary F. (CMS/OC)" <[Gary.Slavinsky@cms.hhs.gov](mailto:Gary.Slavinsky@cms.hhs.gov)>, Jon Booth BB <[Jon.Booth@cms.hhs.gov](mailto:Jon.Booth@cms.hhs.gov)>

**Subject:** Re: [Data.Healthcare.gov](http://Data.Healthcare.gov).

We've done a spot check and we aren't displaying PII, although note we don't control or police that on behalf of customers (e.g. an authorized user could publish PII if they wished). With respect to the CAC dataset there are only organizational phone numbers and email addresses (although some appear to be individual email addresses which are listed as the organizational email address).

Let us know what we can do to provide more information or if there's some security concern and we should alert our operations team to be all hands on deck or something.

Joe

**Socrata**

o: 202-747-0024

m: (b)(6)  
joe.pringle@socrata.com

On Mon, Nov 18, 2013 at 4:07 PM, Joe Pringle <joe.pringle@socrata.com> wrote:

I don't think there is any PII on [data.healthcare.gov](http://data.healthcare.gov) but we're also going through the datasets now to check and confirm. I'm also unaware of any security attacks and am also checking that right now.

Joe

**Socrata**

o: 202-747-0024

m: (b)(6)  
joe.pringle@socrata.com

On Mon, Nov 18, 2013 at 4:01 PM, Patel, Ketan (CMS/OC) <Ketan.Patel@cms.hhs.gov> wrote:

Joe,

Can you confirm we are not showing any PII information [data.healthcare.gov](http://data.healthcare.gov) or any part of CAC form. Also want to know if there were any security attacks against [data.healthcare.gov](http://data.healthcare.gov) and if we have any PII or account information compromised or not?

Immediate response needed..

Thanks,

Ketan

**Blank Page**

Message

**From:** Schankweiler, Thomas W. [NotResp]  
 on behalf of Schankweiler, Thomas W. (CMS/OIS)  
**Sent:** 12/3/2013 7:24:34 PM  
**To:** Coutts, Todd (CMS/OIS) [NotResp]  
 [NotResp] Garner, John R. (CMS/CMCS) [NotResp]  
 [NotResp] Michael Finkel  
 [mfinkel@qssinc.com]  
**CC:** Grothe, Kirk A. (CMS/OIS) [NotResp]  
 [NotResp] Outerbridge, Monique (CMS/OIS) [NotResp]  
 [NotResp] Lyles, Darrin V. (CMS/OIS) [NotResp]  
 [NotResp] Oh, Mark U.  
 (CMS/OIS) [NotResp]  
 Van, Hung B. (CMS/OIS) [NotResp]  
 [NotResp] Kane, David (CMS/OIS) [NotResp]  
 [NotResp] Fender, Rebecca (CMS/CCSQ) [NotResp]  
**BCC:** 'Ramamoorthy, Balaji Manikandan (CGI Federal)' [balajimanikandan.ramamoorthy@cgifederal.com]; Reinhold, Leslie  
 A. (CMS/OEM) [NotResp]  
**Subject:** RE: [NotResp]

Excellent, Thanks

**From:** Coutts, Todd (CMS/OIS)  
**Sent:** Tuesday, December 03, 2013 1:59 PM  
**To:** Schankweiler, Thomas W. (CMS/OIS); Garner, John R. (CMS/OA); Michael Finkel  
**Cc:** Grothe, Kirk A. (CMS/OIS); Outerbridge, Monique (CMS/OIS); Lyles, Darrin V. (CMS/OIS); Oh, Mark U. (CMS/OIS);  
 Van, Hung B. (CMS/OIS); Kane, David (CMS/OIS); Fender, Rebecca (CMS/CCSQ)  
**Subject:** [NotResp]

Tom,

Please see correction below!

**From:** Coutts, Todd (CMS/OIS)  
**Sent:** Tuesday, December 03, 2013 1:46 PM  
**To:** Schankweiler, Thomas W. (CMS/OIS); Garner, John R. (CMS/CMCS); Michael Finkel  
**Cc:** Grothe, Kirk A. (CMS/OIS); Outerbridge, Monique (CMS/OIS); Lyles, Darrin V. (CMS/OIS); Oh, Mark U. (CMS/OIS);  
 Van, Hung B. (CMS/OIS); Kane, David (CMS/OIS); Fender, Rebecca (CMS/CCSQ)  
**Subject:** RE: [NotResp]

Hi Tom,

We just worked with CGI and it is in testing now. Depending on how the testing looks . . .

- Worst case, it will go into production on 12/9 (Sunday night going into Monday morning)
- Best case, it will go into production on Thursday 12/5 (Wednesday night going into Thursday morning)

Todd Coutts

Centers for Medicare & Medicaid Services

Office of Information Services

301-492-5139 (office) (b)(6) (mobile) | [todd.couts1@cms.hhs.gov](mailto:todd.couts1@cms.hhs.gov)

7700 Wisconsin Ave Bethesda MD 20814 | Location: 9308

**From:** Schankweiler, Thomas W. (CMS/OIS)

**Sent:** Tuesday, December 03, 2013 8:34 AM

**To:** Coutts, Todd (CMS/OIS); Garner, John R. (CMS/OA); Michael Finkel

**Cc:** Grothe, Kirk A. (CMS/OIS); Outerbridge, Monique (CMS/OIS); Lyles, Darrin V. (CMS/OIS); Oh, Mark U. (CMS/OIS); Van, Hung B. (CMS/OIS); Kane, David (CMS/OIS)

**Subject:** RE: (b)(6) NotResp

Todd, Chip, and Mike

Can we get this coordinated for implementation tonight or on Wed at the latest? Which includes coordination with SERCO.

We have security testing beginning on Monday for FFM and SERCO, and it would be ideal if this fix was in place. We also have a number of open items with the department and DHS which are awaiting this fix action to go in place.

Thanks,

Tom

**From:** Fender, Rebecca (CMS/CCSQ)

**Sent:** Tuesday, November 26, 2013 7:18 PM

**To:** Schankweiler, Thomas W. (CMS/OIS)

**Subject:** (b)(6) NotResp

Let me know if you need anything else. I'm not opposed to any direction but I do want it coordinated and I do want to make sure leadership isn't upset and frustrated if SERCO goes down. Honestly if I was picking between the two I would pick to fix the PII. It's a broader issue in my book. Just my humble opinion.

Becky Fender PMP®

CMS

Cell: (b)(6)

Office 410-786-1006

**From:** Schankweiler, Thomas W. (CMS/OIS)

**Sent:** Tuesday, November 26, 2013 6:57 PM

**To:** Fender, Rebecca (CMS/CCSQ); Outerbridge, Monique (CMS/OIS); Basavaraju, Venkat (CMS/OIS)

**Cc:** Grothe, Kirk A. (CMS/OIS); Oh, Mark U. (CMS/OIS); Van, Hung B. (CMS/OIS); Margush, Doug C. (CMS/OIS); Coutts, Todd (CMS/OIS); Lyles, Darrin V. (CMS/OIS); Fletcher, John A. (CMS/OIS)

**Subject:** (b)(6) NotResp

Here is my concern. This change will also effect the way consumers pull data. If we launch and we get a drove of people show up on the 30th and their are presented with exposure of PII, we will have a very bad situation on our hands. So

now we are faced with the possibility that Serco could be down for days, when it MUST be up, and the possibility of exposing PII and experiencing a new round of political attacks.

I think if we coordinate decisively that we can all make this work. It would mean identifying a roll-back plan, and implementing the changes on Friday morning, testing by SERCO, and rolling-back quickly if it is not successful. I am not sure what all would need to happen to make this happen, but I think we need to launch on the 30th with a reduced risk of PII exposure; that should be the goal.

I'll be on the 9pm call, and hope maybe we can talk about this near the conclusion of the call.

Thanks,

Tom

---

**From:** Fender, Rebecca (CMS/CCSQ)

**Sent:** Tuesday, November 26, 2013 6:28 PM

**To:** Schankweiler, Thomas W. (CMS/OIS); Outerbridge, Monique (CMS/OIS); Basavaraju, Venkat (CMS/OIS)

**Cc:** Grothe, Kirk A. (CMS/OIS); Oh, Mark U. (CMS/OIS); Van, Hung B. (CMS/OIS); Margush, Doug C. (CMS/OIS); Coutts, Todd (CMS/OIS); Lyles, Darrin V. (CMS/OIS); Fletcher, John A. (CMS/OIS)

**Subject:** [REDACTED] NotResp

Hi All,

I just had a quick call with Tom. I am attaching a document I asked CGI to put together a few days ago when this first came to my attention. Again, I agree this needs to take place and is very important but each time we do something with URLs/Servers or Logins we are down for many days with Serco. In fact we were down today due to changes EIDM made. We need to make sure our timing is coordinated(across all contractors), we have appropriate resources available, a rollback plan and possibly do it after hours/early morning. Whatever timing is decided, we need to make sure all leadership understands the risks to doing it (taking SERCO down) and not doing it (exposing PII). I'm not sure something prior to the 30<sup>th</sup> and our immediate push to clear [REDACTED] NotResp [REDACTED] ell with this effort. I will leave it to the group to make recommendations to leadership on timing and priorities.

Defect numbers are in CALT: artf161121 / artf161124 and this is part of the List of 65, it is N3 which again was identified to better secure [REDACTED] NotResp [REDACTED] you have further concerns/questions please reach out to Tom Schankweiler.

To Test: Go through normal process as an ESW while someone from our security team is in the backend ensures that [REDACTED] NotResp [REDACTED] e. When an ESW closes a completed application) and creates [REDACTED] NotResp [REDACTED] when they search and choose another application to work on or when they click the "Create Application" link.

Let me know if you have questions.

Becky

Becky Fender PMP®

CMS

Cell [REDACTED] (b)(6)

Office 410-786-1006



**From:** Schankweiler, Thomas W. (CMS/OIS)

**Sent:** Tuesday, November 26, 2013 5:19 PM

**To:** Outerbridge, Monique (CMS/OIS); Basavaraju, Venkat (CMS/OIS); Fender, Rebecca (CMS/CCSQ)

**Cc:** Grothe, Kirk A. (CMS/OIS); Oh, Mark U. (CMS/OIS); Van, Hung B. (CMS/OIS); Margush, Doug C. (CMS/OIS); Coutts, Todd (CMS/OIS); Lyles, Darrin V. (CMS/OIS); Fletcher, John A. (CMS/OIS)

**Subject:** [Redacted] NotResp

Did this get resolved today? I can participate in a call later tonight.

Tom

**From:** Schankweiler, Thomas W. (CMS/OIS)

**Sent:** Tuesday, November 26, 2013 12:47 PM

**To:** Fender, Rebecca (CMS/CCSQ); Outerbridge, Monique (CMS/OIS); Basavaraju, Venkat (CMS/OIS)

**Cc:** Grothe, Kirk A. (CMS/OIS); Oh, Mark U. (CMS/OIS); Van, Hung B. (CMS/OIS); Margush, Doug C. (CMS/OIS); Coutts, Todd (CMS/OIS); Lyles, Darrin V. (CMS/OIS) ([Darrin.Lyles@cms.hhs.gov](mailto:Darrin.Lyles@cms.hhs.gov)); Fletcher, John A. (CMS/OIS)

**Subject:** [Redacted] NotResp

Rebecca and Monique,

I am inclined to say yes we need this fix put in place. The fix is intended to resolve a serious issue where data, which is not a consumers, is showing up in searches and in xqueries. This is starting to result in a high number of security and privacy incidents, and has a public view to it. We should have a quick meeting about this so CMS can make a final determination. Maybe it could come down, if needed, during this weekend to allow for the test?

Also I am not sure why testing can only be done in prod? Can't another set of self-signed certificates be issued to address this? or is it the case where there is not a matching environment to perform the testing in?

Tom

**From:** Fender, Rebecca (CMS/CCSQ)

**Sent:** Tuesday, November 26, 2013 10:52 AM

**To:** Schankweiler, Thomas W. (CMS/OIS); Outerbridge, Monique (CMS/OIS); Basavaraju, Venkat (CMS/OIS)

**Subject:** [Redacted] NotResp

**Importance:** High

Hi Tom and Monique,

I have serious concerns about this "fix". Every time we do something with the URL we are down for days at SERCO. We can only test this in PROD due to the [Redacted] NotResp that goes to EIDM and gets passed to ESD. Can you all let me know if you feel we need to take the risk of SERCO being down for a few days? Trust me when I say there is lots of pressure and focus on SERCO and any downtime they incur due to a CGI fix.

Becky

Becky Fender PMP®

CMS

Cell: [Redacted] (b)(6)

Office 410-786-1006

**From:** Fender, Rebecca (CMS/CCSQ)

**Sent:** Tuesday, November 26, 2013 10:48 AM

**To:** 'O'Mara, Katyanne J (CGI Federal)'; Minze Chien; Venky Natarajan; Basavaraju, Venkat (CMS/OIS); Niranjan Santhamoorthy; [greg.greshman.health@gmail.com](mailto:greg.greshman.health@gmail.com); Nitin Matta; Girish Shetty; Sundar, Raj N (CGI Federal); Thangavelu, Raja (Non-Member); Ivan Vinogradov; Ramamoorthy, Balaji Manikandan (CGI Federal); Anbu, Bala (Non-Member); Cecilio, Sal (CGI Federal); Roche, Jacqueline R. (CMS/CCIIO)

**Subject:** [REDACTED] NotResp

I still do not feel that this is urgent and must happen as a priority. I will discuss with Tom and Monique. I do agree it should happen but I know this will take us down for several days and that simply can't happen at this time. There is NO way to test this other than in prod due to the [REDACTED] NotResp

Becky Fender PMP®

CMS

Cell [REDACTED] (b)(6)

Office 410-786-1006

**From:** O'Mara, Katyanne J (CGI Federal) [<mailto:katyanne.omara@cgifederal.com>]

**Sent:** Tuesday, November 26, 2013 10:45 AM

**To:** Fender, Rebecca (CMS/CCSQ); Minze Chien; Venky Natarajan; Basavaraju, Venkat (CMS/OIS); Niranjan Santhamoorthy; [greg.greshman.health@gmail.com](mailto:greg.greshman.health@gmail.com); Nitin Matta; Girish Shetty; Sundar, Raj N (CGI Federal); Thangavelu, Raja (Non-Member); Ivan Vinogradov; Ramamoorthy, Balaji Manikandan (CGI Federal); Anbu, Bala (Non-Member); Cecilio, Sal (CGI Federal); Roche, Jacqueline R. (CMS/CCIIO)

**Subject:** [REDACTED] NotResp

Hi Becky,

I understand your concern.

Defect numbers are in CALT: artf161121 / artf161124 and this is part of the List of 65, it is N3 which again was identified to better secure [REDACTED] NotResp If you have further concerns/questions please reach out to Tom Shankweiler.

To Test: Go through normal process as an ESW while someone from our security team is in the backend ensures that

[REDACTED] NotResp

ie. When an ESW closes a completed application) and creates

[REDACTED] NotResp

then they search and choose another application to work on or when they click the "Create Application" link.

Soumya, Manisha, Eddie and others, even Shaina can be part of the front end testing and Balaji will be assigning someone from his security team to work with us in a coordinated testing effort tomorrow to confirm that the sessions are being created and cleared appropriately.

Our Ops and Security team have completed their tasks. Sal will complete his tasks today. I just need confirmation from EIDM team that they made their change. We will be ready for the coordinated test tomorrow.

I will update the document I sent out with this information.

I hope this answers your questions and alleviates your concerns regarding testing. This is about closing the loop on open sessions, not changing your workflow or affecting your current workflow it's about making your current sessions more secure.

Thanks,  
KO

Katy O'Mara | Manager | Health and Compliance Group | CGI Federal  
W: 703-227-6411 | C: (b)(6) | [www.cgi.com](http://www.cgi.com)

**From:** Fender, Rebecca (CMS/CCSQ) [<mailto:Rebecca.Fender@cms.hhs.gov>]

**Sent:** Tuesday, November 26, 2013 9:58 AM

**To:** O'Mara, Katyanne J (CGI Federal); Minze Chien; Venky Natarajan; Venkat.Basavaraju; Niranjan Santhamoorthy; [greg.greshman.health@gmail.com](mailto:greg.greshman.health@gmail.com); Nitin Matta; Girish Shetty; Sundar, Raj N (CGI Federal); Thangavelu, Raja (Non-Member); Ivan Vinogradov; Ramamoorthy, Balaji Manikandan (CGI Federal); Anbu, Bala (Non-Member); Cecilio, Sal (CGI Federal); Roche, Jacqueline R. (CMS/CCIIO)

**Subject:** NotResp

I will try to call in later but have a conflicting meeting with NPC and leadership about the notices issues. Sorry. I really do NOT want to move forward with this until I understand how we plan to test and why this is such a rush as well as how it was discovered. As we know from past experience changes like this can keep SERCO down for days and we cannot afford that at this time.

Becky Fender PMP®  
CMS  
Cell: (b)(6)  
Office 410-786-1006

-----Original Appointment-----

**From:** O'Mara, Katyanne J (CGI Federal) [<mailto:katyanne.omara@cgifederal.com>]

**Sent:** Monday, November 25, 2013 4:20 PM

**To:** O'Mara, Katyanne J (CGI Federal); Minze Chien; Venky Natarajan; Basavaraju, Venkat (CMS/OIS); Niranjan Santhamoorthy; [greg.greshman.health@gmail.com](mailto:greg.greshman.health@gmail.com); Nitin Matta; Girish Shetty; Sundar, Raj N (CGI Federal); Thangavelu, Raja (Non-Member); Ivan Vinogradov; Ramamoorthy, Balaji Manikandan (CGI Federal); Anbu, Bala (Non-Member); Cecilio, Sal (CGI Federal); Fender, Rebecca (CMS/CCSQ); Roche, Jacqueline R. (CMS/CCIIO)

**Subject:** NotResp

**When:** Tuesday, November 26, 2013 10:00 AM-10:30 AM (UTC-05:00) Eastern Time (US & Canada).

**Where:** dial: (b)(6)

Hi Everyone,

I'd like to get an update on the tasks below and ensure we are on target for completion for tomorrow afternoon for testing to begin tomorrow night or Wednesday morning in Test 2.

Detailed Technical Action Items:

#### EIDM Team Tasks

1. Currently EIDM is protecting the URL [NotResp] Change the policy to protect the following URL pattern [NotResp]
2. All the header variables remains the same. (NO CHANGES REQUIRED)

[NotResp]

#### FFM Ops Team Tasks

1. Add the following RP rules for the English

[NotResp]

2. Restart the Apache RP for the English

#### FFM Security Team Tasks

[NotResp]

#### Application Team Tasks

1. Do a ping to [NotResp] every 10 or 15 minutes to keep the EIDM [NotResp] live from the main ESD page. (Please get the guidance from Jeremy)
2. Currently in the [NotResp] page when the ESD worker searches for an [NotResp] and clicks on the link, it takes the user to the IndividualApp. Instead do a HTTP POST to https [NotResp] the HTTP POST Parameter should be

[NotResp]

Message

**From:** Schankweiler, Thomas W. (CMS/OIS) [NotResp]  
[NotResp]  
on behalf of Schankweiler, Thomas W. (CMS/OIS)  
**Sent:** 12/4/2013 2:59:54 AM  
**To:** 'Goodrich, Lynn F (CGI Federal)' [lynn.goodrich@cgifederal.com]  
**Subject:** RE: Security Items that Need Attention

THANK YOU!!!

**From:** Goodrich, Lynn F (CGI Federal) [mailto:lynn.goodrich@cgifederal.com]  
**Sent:** Tuesday, December 03, 2013 9:21 PM  
**To:** Outerbridge, Monique (CMS/OIS); Kane, David (CMS/OIS); Coutts, Todd (CMS/OIS); Schankweiler, Thomas W. (CMS/OIS); mfinkel@qssinc.com; sbanks@foregroundsecurity.com; Warren, Kevin (CMS/OIS); Fletcher, John A. (CMS/OIS); Van, Hung B. (CMS/OIS); Grothe, Kirk A. (CMS/OIS); Lyles, Darrin V. (CMS/OIS); vnatarajan@qssinc.com; Kirk, Thomas (GSS-CGI); Martin, Rich (CGI Federal)  
**Cc:** [NotResp]  
**Subject:** RE: Security Items that Need Attention

Please find attached a detailed update of the Remedy tickets referenced in #2 below as well as some additional ones opened that day missing from the list.

Please let me know if you have any questions.

Thanks.

**Lynn Goodrich**  
IT Security Manager | CGI Federal Health & Compliance Security Practice (HCSP) | Cell (b)(6) | Office: 703-227-5568 | [Lynn.Goodrich@cgifederal.com](mailto:Lynn.Goodrich@cgifederal.com)

CONFIDENTIALITY NOTICE: Proprietary/Confidential Information belonging to CGI Group Inc. 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 email.

**From:** Martin, Rich (CGI Federal)  
**Sent:** Tuesday, December 03, 2013 9:17 AM  
**To:** Krishnan, Venkatesh (CGI Federal); Goodrich, Lynn F (CGI Federal)  
**Cc:** Ramamoorthy, Balaji Manikandan (CGI Federal)  
**Subject:** FW: Security Items that Need Attention

Hi folks – please see below email trail. There are a number of security incidents/defects various people at CMS are seeking updates for? Can you please verify those remedy numbers and determine which are defects assigned to us and which are POAMs. Also, we can use this as the basis for or status report internally and ultimately to CMS – all will want a dashboard backed up by detail list. Please let me know ASAP. Thank you.

**From:** Kirk, Thomas (GSS-CGI)  
**Sent:** Tuesday, December 03, 2013 8:09 AM  
**To:** Martin, Rich (CGI Federal)  
**Subject:** FW: Security Items that Need Attention

CMS001030

Tom Kirk | Government Secure Solutions CGI Inc. (b)(6) cell | tom.kirk@cgifederal.com

**From:** Outerbridge, Monique (CMS/OIS) [mailto:monique.outerbridge@cms.hhs.gov]

**Sent:** Tuesday, December 03, 2013 8:07 AM

**To:** Ramamoorthy, Balaji Manikandan (CGI Federal); Kane, David (CMS/OIS); Coutts, Todd (CMS/OIS); Schankweiler, Thomas W. (CMS/OIS); Michael Finkel; sbanks@foregroundsecurity.com

**Cc:** Warren, Kevin (CMS/OIS); Fletcher, John A. (CMS/OIS); Van, Hung B. (CMS/OIS); Grothe, Kirk A. (CMS/OIS); Lyles, Darrin V. (CMS/OIS); 'Venky Natarajan' (vnatarajan@qssinc.com) (vnatarajan@qssinc.com); Goodrich, Lynn F (CGI Federal); Kirk, Thomas (GSS-CGI)

**Subject:** RE: Security Items that Need Attention

Hey guys. Has this security issue been resolved yet? This is very important and needs to happen asap.

---

**From:** Ramamoorthy, Balaji Manikandan (CGI Federal) [balajimanikandan.ramamoorthy@cgifederal.com]

**Sent:** Wednesday, November 27, 2013 2:48 PM

**To:** Kane, David (CMS/OIS); Coutts, Todd (CMS/OIS); Schankweiler, Thomas W. (CMS/OIS); Michael Finkel; sbanks@foregroundsecurity.com

**Cc:** Warren, Kevin (CMS/OIS); Fletcher, John A. (CMS/OIS); Van, Hung B. (CMS/OIS); Grothe, Kirk A. (CMS/OIS); Lyles, Darrin V. (CMS/OIS); 'Venky Natarajan' (vnatarajan@qssinc.com) (vnatarajan@qssinc.com); Goodrich, Lynn F (CGI Federal); Kirk, Thomas (GSS-CGI); Outerbridge, Monique (CMS/OIS)

**Subject:** RE: Security Items that Need Attention

Including Stacy Banks.

Thanks

Balaji M. Ramamoorthy

**From:** Kane, David (CMS/OIS) [mailto:David.Kane@cms.hhs.gov]

**Sent:** Wednesday, November 27, 2013 2:35 PM

**To:** Todd.Coutts1; Schankweiler, Thomas W. (CMS/OIS); Michael Finkel

**Cc:** Warren, Kevin (CMS/OIS); Fletcher, John A. (CMS/OIS); Van, Hung B. (CMS/OIS); kirk.grothe; Lyles, Darrin V. (CMS/OIS); 'Venky Natarajan' (vnatarajan@qssinc.com) (vnatarajan@qssinc.com); Goodrich, Lynn F (CGI Federal); Kirk, Thomas (GSS-CGI); Ramamoorthy, Balaji Manikandan (CGI Federal); monique.outerbridge

**Subject:** RE: Security Items that Need Attention

Todd,

Did we receive a response indicating the status of each? Please advise.

Respectfully,

DAVID KANE

Office: 410-786-1193

BB: (b)(6)

David.Kane@cms.hhs.gov

**From:** Coutts, Todd (CMS/OIS)

**Sent:** Tuesday, November 26, 2013 3:48 PM

**To:** Schankweiler, Thomas W. (CMS/OIS); Kane, David (CMS/OIS); Michael Finkel

**Cc:** Warren, Kevin (CMS/OIS); Fletcher, John A. (CMS/OIS); Van, Hung B. (CMS/OIS); Grothe, Kirk A. (CMS/OIS); Lyles, Darrin V. (CMS/OIS); 'Venky Natarajan' ([vnatarajan@qssinc.com](mailto:vnatarajan@qssinc.com)) ([vnatarajan@qssinc.com](mailto:vnatarajan@qssinc.com)); [lynn.goodrich@cgifederal.com](mailto:lynn.goodrich@cgifederal.com); [Thomas.Kirk@gss-cgi.com](mailto:Thomas.Kirk@gss-cgi.com); 'Ramamoorthy, Balaji Manikandan (CGI Federal)' ([balajimanikandan.ramamoorthy@cgifederal.com](mailto:balajimanikandan.ramamoorthy@cgifederal.com)); Outerbridge, Monique (CMS/OIS)

**Subject:** Security Items that Need Attention

QSSI and CGI,

I am writing to highlight several security incidents that need your attention. As they are security issues, please consider the Remedy ticket your authorization to act. I am only sending the Remedy numbers to avoid transmitting too much detail. By tomorrow, please communicate back to use their status (closed, in process, etc) and at least a tentative date for resolution.

1. These are the two that Tom Schankweiler raised today.
  - INC000002589982
  - artf161265 INC2598675
2. Additionally, we identified several open tickets in Remedy.
  - 2614246
  - 2614253
  - 2614255
  - 2614297
  - 2614299
  - 2614303
  - 2614304
  - 2614305
  - 2614307
  - 2614309
  - 2614310
  - 2614311
  - 2614313
  - 2614316
  - 2614317
  - 2614318
  - 2614319
  - 2614320
  - 2614321
  - 2614322
  - 2614323
  - 2614324
  - 2614325
  - 2614326
  - 2614328
  - 2614329
  - 2614330
  - 2614331
  - 2614332
  - 2614327
  - 2614333
  - 2614334
  - 2614335
  - 2614336
  - 2614337



- 2614338
- 2614339
- 2614340
- 2614341

**Todd Coutts**

Centers for Medicare & Medicaid Services

Office of Information Services

301-492-5139 (office) | (b)(6) (mobile) | [todd.couts1@cms.hhs.gov](mailto:todd.couts1@cms.hhs.gov)

7700 Wisconsin Ave Bethesda MD 20814 | Location: 9308

**From:** Schankweiler, Thomas W. (CMS/OIS)

**Sent:** Tuesday, November 26, 2013 12:41 PM

**To:** Coutts, Todd (CMS/OIS); Kane, David (CMS/OIS); Michael Finkel

**Cc:** Warren, Kevin (CMS/OIS); Fletcher, John A. (CMS/OIS); Van, Hung B. (CMS/OIS); Grothe, Kirk A. (CMS/OIS); Lyles, Darrin V. (CMS/OIS)

**Subject:** INC000002589982 Need details regarding (b)(6) NotResp

Todd,

I would like to escalate this ticket NC000002589982 as being high risk on the defect list. I know that a bunch of security risk have recently appeared on the list but I wanted to let you know this one is considered high priority. In total we now have two tickets that are considered high priority. Contact me if you have any questions.

Thanks,

Tom

**From:** Ramamoorthy, Balaji Manikandan (CGI Federal) [<mailto:balajimanikandan.ramamoorthy@cgifederal.com>]

**Sent:** Tuesday, November 26, 2013 10:52 AM

**To:** Schankweiler, Thomas W. (CMS/OIS); Willard, Adam (CMS/CTR)

**Cc:** Warren, Kevin (CMS/OIS); Quaintance, Eric (CGI Federal); Dhas, Navin (CGI Federal); Alford, Justin (CGI Federal); Martin, Rich (CGI Federal)

**Subject:** RE: artf160711 / INC000002589982 Need details regarding (b)(6)

Hi Tom,

We promoted the code fix into production. Apparently the security enforcement is turned off.

The Alfresco documents (notices) that are saved are not having the proper meta data populated to turn on the enforcements. So in addition to the fix that has been rolled in the following actions needs to occur.

1. Do a manual batch job to update the meta data for all the existing notices.
2. Have the developers fix the code so that any new notices that are saved has the proper metadata for enforcement.

These 2 action items are being coordinated internally right now. We don't have an ETA yet.

Thanks

Balaji M. Ramamoorthy



**From:** Schankweiler, Thomas W. (CMS/OIS) [mailto:thomas.schankweiler@cms.hhs.gov]

**Sent:** Tuesday, November 26, 2013 10:42 AM

**To:** Ramamoorthy, Balaji Manikandan (CGI Federal); Willard, Adam (CMS/CTR)

**Cc:** Warren, Kevin (CMS/OIS); Quaintance, Eric (CGI Federal); Dhas, Navin (CGI Federal)

**Subject:** artf160711 / INC000002589982 Need details regarding

NotResp

Balaji, Adam, and Kevin

I am looking for an update on this ticket. Can someone provide be a status of where we are with this item? Has it been corrected? Is the situation still occurring?

Thanks,

Tom

**From:** Ramamoorthy, Balaji Manikandan (CGI Federal) [mailto:balajimanikandan.ramamoorthy@cgifederal.com]

**Sent:** Wednesday, November 06, 2013 12:39 PM

**To:** Willard, Adam (CMS/CTR)

**Cc:** Warren, Kevin (CMS/OIS); Schankweiler, Thomas W. (CMS/OIS); Quaintance, Eric (CGI Federal); Dhas, Navin (CGI Federal)

**Subject:** RE: Need details regarding

NotResp

Hi Adam,

There are multiple instances of NotResp We expect NotResp guarantees for the uniqueness across JVM's. We did go this route to see if there were duplicates.

So far the root cause has not been determined for the notices. In this particular instance we did see that the username were closely identical between the user1 and user2. There was a special character "-" at the end (and that was the only difference). We are also looking into the NotResp Xquery to see how it behaves and whether it has to be tweaked.

Thanks

Balaji M. Ramamoorthy

**From:** Willard, Adam (CMS/CTR) [mailto:Adam.Willard@cms.hhs.gov]

**Sent:** Wednesday, November 06, 2013 12:05 PM

**To:** Ramamoorthy, Balaji Manikandan (CGI Federal)

**Cc:** Warren, Kevin (CMS/OIS); Schankweiler, Thomas W. (CMS/OIS); Quaintance, Eric (CGI Federal); Dhas, Navin (CGI Federal)

**Subject:** RE: Need details regarding

NotResp

Is Alfresco just 1 instance or are there several instances in production? If there are multiple systems generating a NotResp there could be collisions.

What was the analysis from the Users who said they saw someone's Notice instead of theirs. Was there any check to see if the NotResp for that user and the other user was the same?

**Adam Willard** (Contractor)  
703-354-2229 x513 (Direct)

(b)(6) (Mobile)

Adam.Willard@cms.hhs.gov

**CMS Re: Security Team**  
Consumer Information & Insurance Systems Group (CIISG)  
Centers for Medicare & Medicaid Services (CMS)  
703-594-4961/ **NotResp**  
[ciisg-soc@cms.hhs.gov](mailto:ciisg-soc@cms.hhs.gov)

---

**From:** Ramamoorthy, Balaji Manikandan (CGI Federal) [balajimanikandan.ramamoorthy@cgifederal.com]  
**Sent:** Wednesday, November 06, 2013 11:47 AM  
**To:** Willard, Adam (CMS/CTR)  
**Cc:** Warren, Kevin (CMS/OIS); Schankweiler, Thomas W. (CMS/OIS); Quaintance, Eric (CGI Federal); Dhas, Navin (CGI Federal)  
**Subject:** RE: Need details regarding **NotResp**  
Hi Adam,

The eligibility notices are stored in Alfresco and the URI's for the notices are stored against the user record in

**NotResp**

The GUID for the PDF document itself is generated by Alfresco and it is sufficiently random.

We did identify this issue internally and it is in the list of high priority items to be fixed. I will track down on the ETA for the fix and let you know.

I agree that in the meantime to see if the rate control can be applied to this specific URL.

Thanks  
Balaji M. Ramamoorthy

**From:** Willard, Adam (CMS/CTR) [mailto:Adam.Willard@cms.hhs.gov]  
**Sent:** Wednesday, November 06, 2013 9:37 AM  
**To:** Ramamoorthy, Balaji Manikandan (CGI Federal)  
**Cc:** Warren, Kevin (CMS/OIS); Schankweiler, Thomas W. (CMS/OIS); Quaintance, Eric (CGI Federal)  
**Subject:** Need details regarding **NotResp**  
**Importance:** High

Balaji,

I noticed this morning that it is possible for anyone to run a brute force against healthcare.gov to obtain the results of their eligibility.

I need to know where you are grabbing the file from **NotResp** something else). Is that system publicly accessible?

We need to know if there is anyway to put in permission checking of the workspace url GUID against the list of possible GUIDs for a user.

I sent Shima (an XOC Security Analyst) my eligibility URL and she was able to see my results in PDF format.

We are looking into a Rate Control for the Akamai WAF to block or limit access to this screen if several attempts are made over X period of time.

**Adam Willard** (Contractor)  
703-354-2229 x513 (Direct)  
(b)(6) Mobile)  
[Adam.Willard@cms.hhs.gov](mailto:Adam.Willard@cms.hhs.gov)

**CMS** **NOT Res** **Security Team**

Consumer Information & Insurance Systems Group (CIISG)

Centers for Medicare & Medicaid Services (CMS)

703-594-4961 (b)(6)

[ciisg-soc@cms.hhs.gov](mailto:ciisg-soc@cms.hhs.gov)

Message

**From:** Schankweiler, Thomas W. (CMS/OIS) [NotResp]  
[NotResp]  
on behalf of Schankweiler, Thomas W. (CMS/OIS)  
**Sent:** 10/10/2013 6:08:32 PM  
**To:** Fryer, Teresa M. (CMS/OIS) [NotResp]  
[NotResp]  
**CC:** Ashbaugh, Jason L. (CMS/OIS) [NotResp]  
Linares, George E. (CMS/OIS) [NotResp]  
[NotResp]; Outerbridge, Monique [NotResp]  
[NotResp] Oh, Mark U. (CMS/OIS) [/o=HHS]  
[NotResp] Chao, Henry  
[NotResp] Warren, Kevin (CMS/OIS)  
(Kevin.Warren@cms.hhs.gov) [NotResp]  
[NotResp]  
**Subject:** RE: Admin passwords and insecurity in healthcare.gov

Hello all,

Here is the feedback regarding this inquiry.

**Statement:**

CMS [NotResp] acknowledges the feedback by the security community. Analysis of the code and a review of the operational environment has confirmed that the site is secure and operating with low risk to consumers.

The code that has been reposted to Pastebin and commented on by TrustedSec is intended to be available to the public code as it makes the user interface (UI) of the site function. By design, these "resource bundles" contain all of the non-personalized text the user will see throughout the site. There is no admin level ID's or passwords located within the [NotResp] posted on-line. The code base at [NotResp] has also just been queried for strings such as "admin password" and "abc123gov" per the twitter screenshot. No evidence was located that there is admin credential revealed. The person who retweeted with the abc password is just being humorous.

The [NotResp] and the SCA test team does run all of the tools mentioned in the article. A lot of commented code was removed prior to production, and the need to perform [NotResp] is a roadmap item, in fact it is scheduled for release to the [NotResp] environment tonight. Performing minification requires a lot of testing to ensure the application is not broken during [NotResp] compression. As [NotResp] can be improved they will be release with subsequent builds.

To the other points in the article The marketplace does not use PHP so that is a non-issue. The use of Captcha was considered at one time, but removed to ensure 508-Compliance and to more importantly to remove burden on a consumer as *A Good Consumer Experience* was a design consideration. Also the concept of guessing ID's to see if there is a valid one or not is a known risk. We can look into taking steps at locking down access controls further, but it would negatively effect the user-experience.

Regards,

Tom Schankweiler, CISSP

Information Security Officer, CCIO  
CMS\OIS\CIISG  
Consumer Information and Insurance Systems Group  
410-786-5956 (Balt. Office, N2-13-22)  
(b)(6) (Mobile)

**From:** Charest, Kevin (OS/ASA/OCIO/OIS)  
**Sent:** Thursday, October 10, 2013 12:21 PM  
**To:** Fryer, Teresa M. (CMS/OIS); Schankweiler, Thomas W. (CMS/OIS)  
**Cc:** Baitman, Frank (OS/ASA/OCIO)  
**Subject:** FW: Admin passwords and insecurity in healthcare.gov  
**Importance:** High

Teresa and Tom,

As you can see from the email chain below and the article at the Trustedsec site there are a significant number of concerns being raised here and they do appear to be legitimate even partially.

I need for you to review the current status of imbedded developer comment and ensure that they are removed. If – as is implied below, the admin password is something as absurd as what is in the tweet it be immediately changed and should be changed regularly in accordance with security standards and best practices.

Please let me know that you received this message and will be looking into for validation and remediation as soon as possible.

Kevin

Kevin Charest Ph.D., CISSP, PMP  
Chief Information Security Officer  
U.S. Department of Health and Human Services

Email: [Kevin.Charest@hhs.gov](mailto:Kevin.Charest@hhs.gov)

NotResp

Ofc. 202-690-5548; Mobile: (b)(6)

*“Driving secure solutions through innovation and sustainable business practices”*

**From:** (b)(6)  
**Sent:** Thursday, October 10, 2013 12:12 PM  
**To:** Charest, Kevin (OS/ASA/OCIO/OIS)

**Cc:** (b)(6)

(b)(6)

**Subject:** Admin passwords and insecurity in healthcare.gov

**Importance:** High

Kevin,

NotResp



**TrustedSec** @TrustedSec

2h

Is the Affordable Health Care Website Secure? Probably not.

[trustedsec.com/october\\_2013/a...](http://trustedsec.com/october_2013/a...) #TrustedSec

Collapse

Reply Retweet Favorite More

**22**

RETWEETS

**3**

FAVORITES

(b)(6)

6:40 AM - 10 Oct 13 · Details

(b)(6)

(b)(6)

45m

comments in tha

NotResp

Details

(b)(6)

Message

**From:** Schankweiler, Thomas W. (CMS/OIS) [NotResp]  
 [NotResp]  
 on behalf of Schankweiler, Thomas W. (CMS/OIS)  
**Sent:** 10/10/2013 6:09:01 PM  
**To:** Villar, Manuel (CMS/CTR) [NotResp]  
 [NotResp]  
**Subject:** FW: Admin passwords and insecurity in healthcare.gov

**From:** Schankweiler, Thomas W. (CMS/OIS)  
**Sent:** Thursday, October 10, 2013 2:09 PM  
**To:** Fryer, Teresa M. (CMS/OIS)  
**Cc:** Ashbaugh, Jason L. (CMS/OIS); Linares, George E. (CMS/OIS); Outerbridge, Monique (CMS/OIS); Oh, Mark U. (CMS/OIS); Chao, Henry (CMS/OIS); Warren, Kevin (CMS/OIS) (Kevin.Warren@cms.hhs.gov)  
**Subject:** RE: Admin passwords and insecurity in healthcare.gov

Hello all,

Here is the feedback regarding this inquiry.

**Statement:**

CMS [NotResp] acknowledges the feedback by the security community. Analysis of the code and a review of the operational environment has confirmed that the site is secure and operating with low risk to consumers.

The code that has been reposted to Pastebin and commented on by TrustedSec is intended to be available to the public code as it makes the user interface (UI) of the site function. By design, these "resource bundles" contain all of the non-personalized text the user will see throughout the site. There is no admin level ID's or passwords located within the [NotResp] posted on-line. The code base at [NotResp] has also just been queried for strings such as "admin password" and "abc123gov" per the twitter screenshot. No evidence was located that there is admin credential revealed. The person who retweeted with the abc password is just being humorous.

The [NotResp] and the SCA test team does run all of the tools mentioned in the article. A lot of commented code was removed prior to production, and the need to perform [NotResp] is a roadmap item, in fact it is scheduled for release to the [NotResp] environment tonight. Performing minification requires a lot of testing to ensure the application is not broken during [NotResp] compression. As [NotResp] can be improved they will be release with subsequent builds.

To the other points in the article The marketplace does not use PHP so that is a non-issue. The use of Captcha was considered at one time, but removed to ensure 508-Compliance and to more importantly to remove burden on a consumer as *A Good Consumer Experience* was a design consideration. Also the concept of guessing ID's to see if there is a valid one or not is a known risk. We can look into taking steps at locking down access controls further, but it would negatively effect the user-experience.

Regards,

Tom Schankweiler, CISSP  
Information Security Officer, CCIIO  
CMS\OIS\CIISG  
Consumer Information and Insurance Systems Group  
410-786-5956 (Balt. Office, N2-13-22)  
(b)(6) (Mobile)

**From:** Charest, Kevin (OS/ASA/OCIO/OIS)  
**Sent:** Thursday, October 10, 2013 12:21 PM  
**To:** Fryer, Teresa M. (CMS/OIS); Schankweiler, Thomas W. (CMS/OIS)  
**Cc:** Baitman, Frank (OS/ASA/OCIO)  
**Subject:** FW: Admin passwords and insecurity in healthcare.gov  
**Importance:** High

Teresa and Tom,

As you can see from the email chain below and the article at the Trustedsec site there are a significant number of concerns being raised here and they do appear to be legitimate even partially.

I need for you to review the current status of imbedded developer comment and ensure that they are removed. If – as is implied below, the admin password is something as absurd as what is in the tweet it be immediately changed and should be changed regularly in accordance with security standards and best practices.

Please let me know that you received this message and will be looking into for validation and remediation as soon as possible.

Kevin

Kevin Charest Ph.D., CISSP, PMP  
Chief Information Security Officer  
U.S. Department of Health and Human Services

Email: Kevin.Charest@hhs.gov

NotResp

Ofc. 202-690-5548; Mobile: (b)(6)

*“Driving secure solutions through innovation and sustainable business practices”*

**From:** (b)(6)  
**Sent:** Thursday, October 10, 2013 12:12 PM  
**To:** Charest, Kevin (OS/ASA/OCIO/OIS)

**Cc:** (b)(6)



(b)(6)

**Subject:** Admin passwords and insecurity in healthcare.gov

**Importance:** High

Kevin,

NotResp



**TrustedSec** @TrustedSec

2h

Is the Affordable Health Care Website Secure? Probably not.  
trustedsec.com/october\_2013/a... #TrustedSec

Collapse

Reply Retweet Favorite More

**22**

RETWEETS

**3**

FAVORITES

(b)(6)

6:40 AM - 10 Oct 13 · Details

(b)(6)

(b)(6)

comments in tha

45m

NotResp

Details

(b)(6)

8

Message

**From:** Schankweiler, Thomas W. [NotResp]  
[NotResp]  
on behalf of Schankweiler, Thomas W. (CMS/OIS)  
**Sent:** 10/11/2013 1:47:24 PM  
**To:** James, Brian M. (CMS/CCIIO) [NotResp]  
**CC:** Brackett, Stacie D. (CMS/CCIIO) [NotResp]  
[NotResp] [NotResp] Booth, Jon G. (CMS/OC) [NotResp]  
**Subject:** RE: Admin passwords and insecurity in healthcare.gov

Brian,

Thanks for the additional info. We had an analyst briefly look into this and it did not appear that anything bad could really happen, but if it is old code lingering it probably needs to be pulled down. It just becomes fodder...

Tom

**From:** James, Brian M. (CMS/CCIIO)  
**Sent:** Friday, October 11, 2013 9:44 AM  
**To:** Schankweiler, Thomas W. (CMS/OIS)  
**Cc:** Brackett, Stacie D. (CMS/CCIIO); Booth, Jon G. (CMS/OC)  
**Subject:** FW: Admin passwords and insecurity in healthcare.gov

Tom, 3rd hand report is that this code was inherited from CTAC when the site was transitioned. If that was the case, it may not have been operative by the time of the article. I don't know enough about the particular vulnerability to understand if we really had a problem, or if they just stumbled across residual junk that was partitioned off to where it was harmless. I don't recall hearing about that vulnerability from the first SCAs (which I was involved in), but those were 3 years ago. As you probably recall, Craig was the GTO on the CTAC contract. If people push that deeply, you may need to approach him for answers about the original configuration, but I don't think he has to be drug into it at this point.

Brian James, Director  
Issuer Data Collection & Management Division  
Consumer Support Group, CCIIO  
[brian.james@cms.hhs.gov](mailto:brian.james@cms.hhs.gov)

Centers for Medicare and Medicaid Services (CMS)  
Center for Consumer Information and Insurance  
200 Independence Ave, SW  
Room 733H.02  
Washington, DC 20201

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 fullest extent of the law.

**From:** Shropshire, Richard (CMS/CCIIO)  
**Sent:** Friday, October 11, 2013 8:05 AM  
**To:** Cummings, Duane (CGI Federal); James, Brian M. (CMS/CCIIO)  
**Subject:** RE: Admin passwords and insecurity in healthcare.gov

Correct, OC should take care of it. I wanted to be sure we touched all the bases before responding to Tom.

Thanks.

---

Rusty Shropshire | CSG | CCIIO  
Ph: 301.492.4238 | BB: (b)(6)

**From:** Cummings, Duane (CGI Federal) [mailto:Duane.Cummings@cgifederal.com]  
**Sent:** Friday, October 11, 2013 7:19 AM  
**To:** Shropshire, Richard (CMS/CCIIO); James, Brian M. (CMS/CCIIO)  
**Subject:** RE: Admin passwords and insecurity in healthcare.gov

Hi Rusty,

That may be a vulnerability that exists in the plan finder site. I forwarded the information to the CGI team that has taken ownership of the site. It looks like something that existed before the transition and the code was just migrated when the site was transitioned from CTAC. Is this something OC would now handle or would your group still manage this risk/issue?

Thanks,

---

**Duane Cummings**  
CGI Federal | 12601 Fair Lakes Circle, Va. 22033  
Phone: 703-227-4704 | Email: [duane.cummings@cgifederal.com](mailto:duane.cummings@cgifederal.com)  
Website: [www.cgi.com](http://www.cgi.com)

**From:** Shropshire, Richard (CMS/CCIIO) [mailto:richard.shropshire@cms.hhs.gov]  
**Sent:** Thursday, October 10, 2013 10:53 PM  
**To:** Cummings, Duane (CGI Federal); James, Brian M. (CMS/CCIIO)  
**Subject:** RE: Admin passwords and insecurity in healthcare.gov

What about Eric's email below that states the URL depicted is [finder.healthcare.gov](http://finder.healthcare.gov) (I think it's the last screenshot).

Richard "Rusty" Shropshire  
Issuer Data Collection & Management Division  
CCIIO Consumer Support Group  
ph: 301.492.4238 | bb: (b)(6)  
[richard.shropshire@cms.hhs.gov](mailto:richard.shropshire@cms.hhs.gov)

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 fullest extent of the law.

---

**From:** Cummings, Duane (CGI Federal) [Duane.Cummings@cgifederal.com]  
**Sent:** Thursday, October 10, 2013 7:52 PM  
**To:** James, Brian M. (CMS/CCIIO); Shropshire, Richard (CMS/CCIIO)  
**Subject:** FW: Admin passwords and insecurity in healthcare.gov  
Hi Brian/Rusty,

I am not sure if you already responded to Tom, but the screen shot(s) appear to be of the consumer portal and not anything related to HIOS or the issue portal. I have passed the email along to the FFM/QHP team here at CGI, but not sure if Tom wanted to direct his request to the CMS QHP team.

Thanks,

---

**Duane Cummings**

CGI Federal | 12601 Fair Lakes Circle, Va. 22033

Phone: 703-227-4704 | Email: [duane.cummings@cgifederal.com](mailto:duane.cummings@cgifederal.com)

Website: [www.cgi.com](http://www.cgi.com)

**From:** Schankweiler, Thomas W. (CMS/OIS) [<mailto:thomas.schankweiler@cms.hhs.gov>]

**Sent:** Thursday, October 10, 2013 5:55 PM

**To:** James, Brian M. (CMS/CCIO)

**Cc:** Brackett, Stacie D. (CMS/CCIO); Lyles, Darrin V. (CMS/OIS); Cummings, Duane (CGI Federal)

**Subject:** FW: Admin passwords and insecurity in healthcare.gov

**Importance:** High

Brian,

I need your contractors to look at this as it relates to the finder page and provide a response by noon Friday. This has attention of the HHS CIO, CMS CIO, and the HHS OIG. An initial response has been provided, but I need your feedback on the Finder page.

[https://www.trustedsec.com/october\\_2013/affordable-health-care-website-secure-probably/](https://www.trustedsec.com/october_2013/affordable-health-care-website-secure-probably/) and take a look at the comments to the post pictured below, on twitter (<https://twitter.com/TrustedSec/statuses/388298092971163648>).

Thanks,

Tom

**From:** Quaintance, Eric (CGI Federal) [<mailto:Eric.Quaintance@cgifederal.com>]

**Sent:** Thursday, October 10, 2013 3:42 PM

**To:** Schankweiler, Thomas W. (CMS/OIS)

**Subject:** RE: Admin passwords and insecurity in healthcare.gov

Hi Tom, one add'l bit of information regarding "CKEditor" as referenced here:

[https://www.trustedsec.com/october\\_2013/affordable-health-care-website-secure-probably/](https://www.trustedsec.com/october_2013/affordable-health-care-website-secure-probably/)

The URL depicted in the Google search results specifies **finder.healthcare.gov**. **Finder** is not part of our project.

**Eric Quaintance**

Healthcare & Compliance | Application Security | H&CP Security Practice

x27.4654 / 610.842.5094 | Herndon: near rm3041 | Fairfax: 6th West-001A

**From:** Schankweiler, Thomas W. (CMS/OIS) [<mailto:thomas.schankweiler@cms.hhs.gov>]

**Sent:** Thursday, October 10, 2013 2:14 PM

**To:** Quaintance, Eric (CGI Federal)

**Subject:** Fw: Admin passwords and insecurity in healthcare.gov

Fyi

**From:** Schankweiler, Thomas W. (CMS/OIS)

**Sent:** Thursday, October 10, 2013 02:08 PM

**To:** Fryer, Teresa M. (CMS/OIS)

**Cc:** Ashbaugh, Jason L. (CMS/OIS); Linares, George E. (CMS/OIS); Outerbridge, Monique (CMS/OIS); Oh, Mark U. (CMS/OIS); Chao, Henry (CMS/OIS); Warren, Kevin (CMS/OIS) ([Kevin.Warren@cms.hhs.gov](mailto:Kevin.Warren@cms.hhs.gov))

**Subject:** RE: Admin passwords and insecurity in healthcare.gov

Hello all,

Here is the feedback regarding this inquiry.

**Statement:**

CMS [NotResp] acknowledges the feedback by the security community. Analysis of the code and a review of the operational environment has confirmed that the site is secure and operating with low risk to consumers.

The code that has been reposted to Pastebin and commented on by TrustedSec is intended to be available to the public code as it makes the user interface (UI) of the site function. By design, these "resource bundles" contain all of the non-personalized text the user will see throughout the site. There is no admin level ID's or passwords located within the [NotRes

p] posted on-line. The code base at [NotRe] is also just been queried for strings such as "admin password" and "abc123gov" per the twitter screenshot. No evidence was located that there is admin credential revealed. The person who retweeted with the abc password is just being humorous.

The [NotResp] and the SCA test team does run all of the tools mentioned in the article. A lot of commented code was removed prior to production, and the need to perform [NotResp] is a roadmap item, in fact it is scheduled for release to the [NotRes] environment tonight. Performing minification requires a lot of testing to ensure the application is not broken during [NotRes] compression. . As [NotResp] can be improved they will be release with subsequent builds.

To the other points in the article The marketplace does not use PHP so that is a non-issue. The use of Captcha was considered at one time, but removed to ensure 508-Compliance and to more importantly to remove burden on a consumer as *A Good Consumer Experience* was a design consideration. Also the concept of guessing ID's to see if there is a valid one or not is a known risk. We can look into taking steps at locking down access controls further, but it would negatively effect the user-experience.

Regards,

Tom Schankweiler, CISSP

Information Security Officer, CCIIO

CMS\OIS\CIISG

Consumer Information and Insurance Systems Group

410-786-5956 (Balt. Office, N2-13-22)

[b)(6)] (Mobile)

**From:** Charest, Kevin (OS/ASA/OCIO/OIS)  
**Sent:** Thursday, October 10, 2013 12:21 PM  
**To:** Fryer, Teresa M. (CMS/OIS); Schankweiler, Thomas W. (CMS/OIS)  
**Cc:** Baitman, Frank (OS/ASA/OCIO)  
**Subject:** FW: Admin passwords and insecurity in healthcare.gov  
**Importance:** High

Teresa and Tom,

As you can see from the email chain below and the article at the Trustedsec site there are a significant number of concerns being raised here and they do appear to be legitimate even partially.

I need for you to review the current status of imbedded developer comment and ensure that they are removed. If – as is implied below, the admin password is something as absurd as what is in the tweet it be immediately changed and should be changed regularly in accordance with security standards and best practices.

Please let me know that you received this message and will be looking into for validation and remediation as soon as possible.

Kevin

Kevin Charest Ph.D., CISSP, PMP  
Chief Information Security Officer  
U.S. Department of Health and Human Services

Email: [Kevin.Charest@hhs.gov](mailto:Kevin.Charest@hhs.gov)

NotResp

Ofc. 202-690-5548; Mobile (b)(6)

*“Driving secure solutions through innovation and sustainable business practices”*

**From:** (b)(6)  
**Sent:** Thursday, October 10, 2013 12:12 PM  
**To:** Charest, Kevin (OS/ASA/OCIO/OIS)  
**Cc:** (b)(6)  
(b)(6)  
**Subject:** Admin passwords and insecurity in healthcare.gov  
**Importance:** High

Kevin,

NotResp



**TrustedSec** @TrustedSec

2h

Is the Affordable Health Care Website Secure? Probably not.  
trustedsec.com/october\_2013/a... #TrustedSec

Collapse

Reply Retweet Favorite More

**22**

RETWEETS

**3**

FAVORITES

(b)(6)

6:40 AM - 10 Oct 13 · Details

(b)(6)

(b)(6)

45m

comments in tha

NotResp

Details

(b)(6)

Message

**From:** Schankweiler, Thomas W. (CMS/OIS); [Redacted] NotResp  
[Redacted] NotResp

on behalf of Schankweiler, Thomas W. (CMS/OIS)

**Sent:** 10/11/2013 1:56:28 PM

**To:** Patel, Ketan [Redacted] NotResp  
James, Brian M. (CMS/CCIIO); [Redacted] NotResp  
Brackett, Stacie D. (CMS/CCIIO); [Redacted] NotResp  
[Redacted] NotResp

**CC:** Lyles, Darrin V. [Redacted] NotResp  
[Redacted] NotResp 'Duane.Cummings@cgifederal.com'  
[Redacted] NotResp [Redacted] NotResp  
[Redacted] NotResp

**Subject:** RE: Admin passwords and insecurity in healthcare.gov

Yeah we saw the same thing. Should the page just be pulled down?

**From:** Patel, Ketan (CMS/OC)  
**Sent:** Friday, October 11, 2013 9:53 AM  
**To:** Schankweiler, Thomas W. (CMS/OIS); James, Brian M. (CMS/CCIIO); Brackett, Stacie D. (CMS/CCIIO)  
**Cc:** Lyles, Darrin V. (CMS/OIS); 'Duane.Cummings@cgifederal.com'; Booth, Jon G. (CMS/OC)  
**Subject:** RE: Admin passwords and insecurity in healthcare.gov

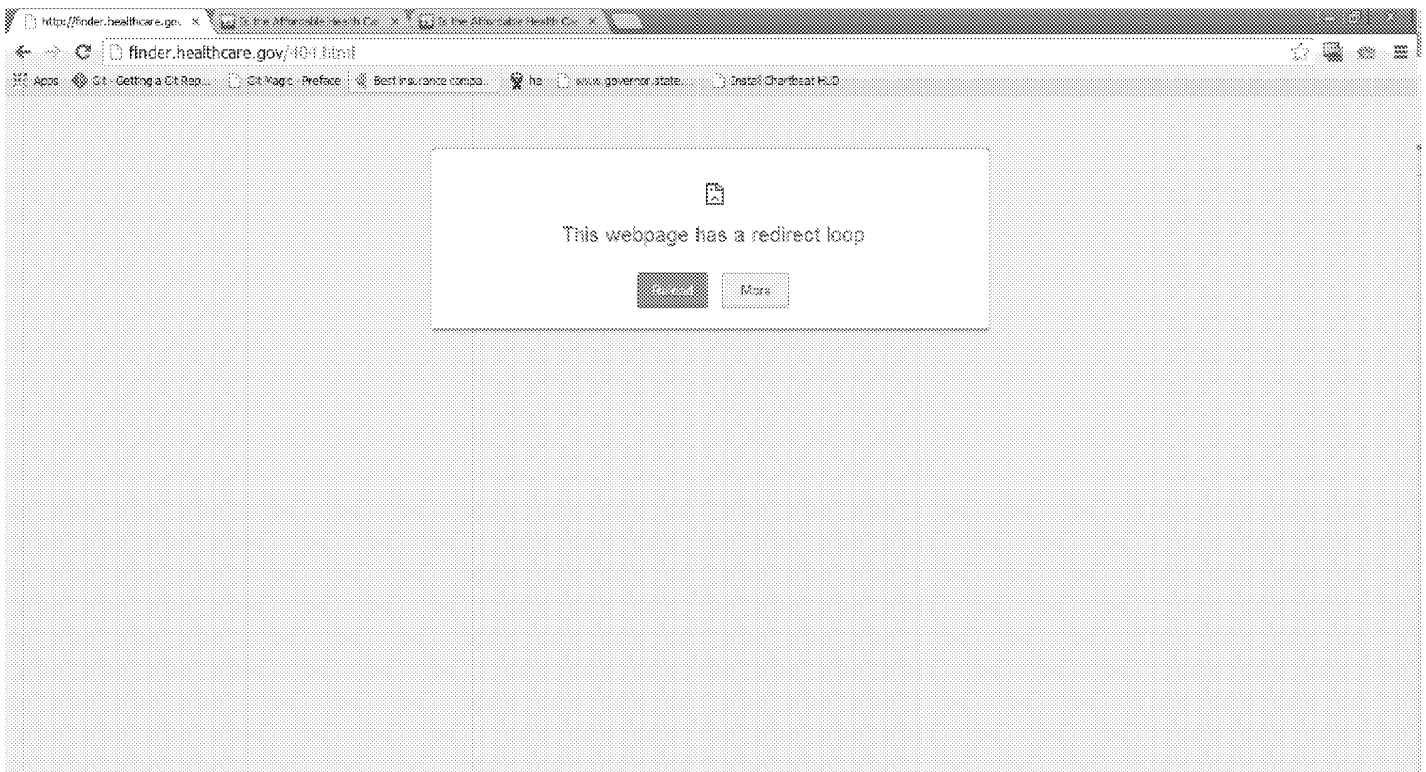
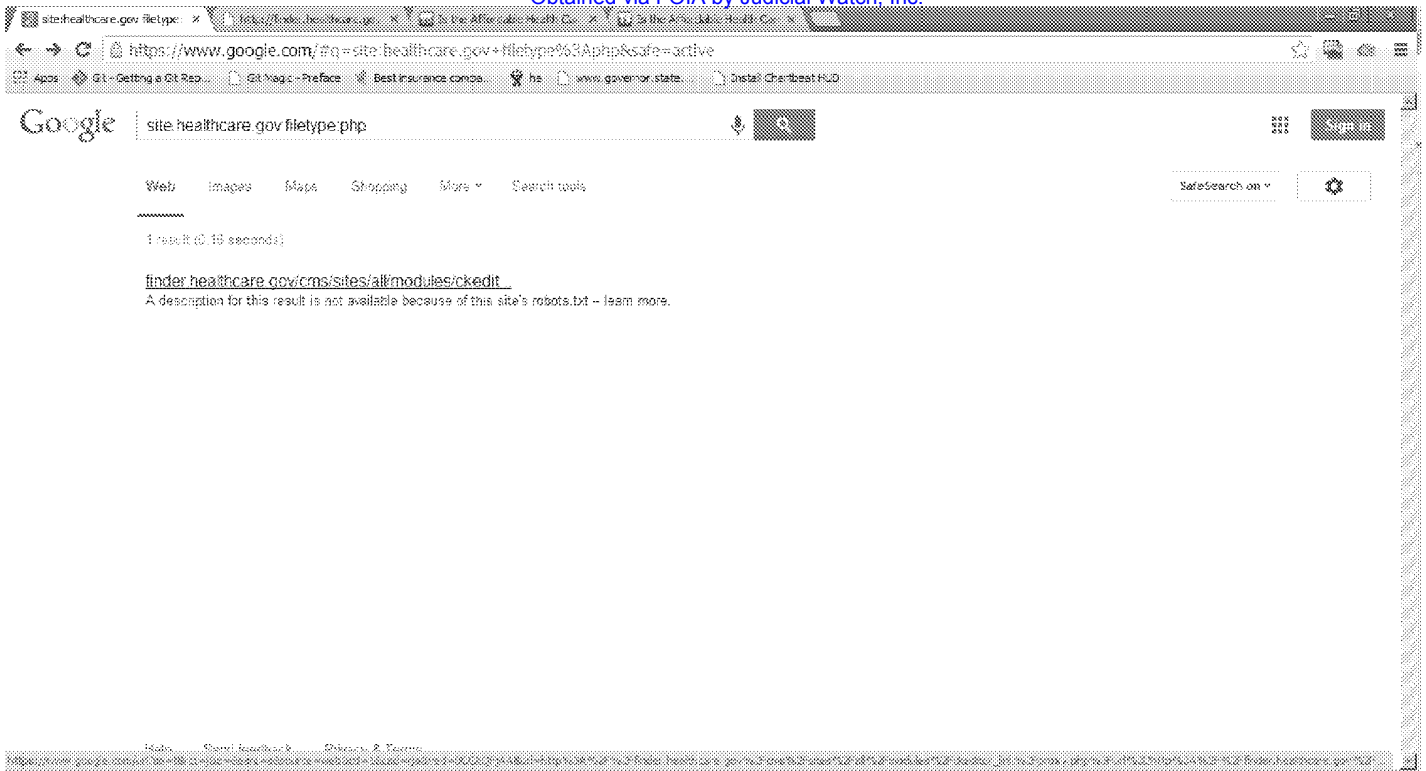
Tom,

Finder.Healthcare.gov was as is migration from department we have done no development on existing Finder Applications. Codebase with no detailed documentation was given to us by HHS. Current Finder application was configured with help from Peter. I just tried below and the

clicked [https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&ved=0CCkQFjAA&url=http%3A%2F%2Ffinder.healthcare.gov%2Fcms%2Fsites%2Fall%2Fmodules%2Fckeditor\\_link%2Fproxy.php%3Furl%3Dhttp%3A%2F%2Ffinder.healthcare.gov%2F&ei=GwBYUpS2GJax4AOE94DYAg&usg=AFQjCNGJDAIclz6MGGZu-pexZkSMfg-dsw](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&ved=0CCkQFjAA&url=http%3A%2F%2Ffinder.healthcare.gov%2Fcms%2Fsites%2Fall%2Fmodules%2Fckeditor_link%2Fproxy.php%3Furl%3Dhttp%3A%2F%2Ffinder.healthcare.gov%2F&ei=GwBYUpS2GJax4AOE94DYAg&usg=AFQjCNGJDAIclz6MGGZu-pexZkSMfg-dsw)

I get 404 page.





**From:** Schankweiler, Thomas W. (CMS/OIS)

**Sent:** Friday, October 11, 2013 9:37 AM

**To:** James, Brian M. (CMS/CCIIO); Brackett, Stacie D. (CMS/CCIIO)

**Cc:** Lyles, Darrin V. (CMS/OIS); 'Duane.Cummings@cgifederal.com'; Booth, Jon G. (CMS/OC); Patel, Ketan (CMS/OC)

**Subject:** RE: Admin passwords and insecurity in healthcare.gov

Brian, Thanks, for some reason I had it in the back of my mind that finder was connected to NotResp

John and Ketan, Could you please review this thread and get back to me by the noon deadline?

Tom

**From:** James, Brian M. (CMS/CCIIO)  
**Sent:** Friday, October 11, 2013 9:35 AM  
**To:** Schankweiler, Thomas W. (CMS/OIS); Brackett, Stacie D. (CMS/CCIIO)  
**Cc:** Lyles, Darrin V. (CMS/OIS); 'Duane.Cummings@cgifederal.com'; Booth, Jon G. (CMS/OC)  
**Subject:** RE: Admin passwords and insecurity in healthcare.gov

Hey Tom, we can have my contractors take a look, but this is the NotResp site... not NotRes<sub>p</sub> This is owned, managed and run by OC, and I don't really have any insight. The person who needs to be made aware of this is Jon Booth (or whoever is operating as his ISSO). I don't mean to pass the buck, and anyone can correct me, but I'm doubtful we have any influence over this. If there is anything my group can do to assist, let me know. We'll pass along any insights provided by our contractors.

Brian James, Director  
Issuer Data Collection & Management Division  
Consumer Support Group, CCIIO  
[brian.james@cms.hhs.gov](mailto:brian.james@cms.hhs.gov)

Centers for Medicare and Medicaid Services (CMS)  
Center for Consumer Information and Insurance  
200 Independence Ave, SW  
Room 733H.02  
Washington, DC 20201

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 fullest extent of the law.

---

**From:** Schankweiler, Thomas W. (CMS/OIS)  
**Sent:** Friday, October 11, 2013 8:57 AM  
**To:** Brackett, Stacie D. (CMS/CCIIO); James, Brian M. (CMS/CCIIO)  
**Cc:** Lyles, Darrin V. (CMS/OIS); 'Duane.Cummings@cgifederal.com'  
**Subject:** RE: Admin passwords and insecurity in healthcare.gov  
Thank you Stacie.

**From:** Brackett, Stacie D. (CMS/CCIIO)  
**Sent:** Friday, October 11, 2013 8:57 AM  
**To:** Schankweiler, Thomas W. (CMS/OIS); James, Brian M. (CMS/CCIIO)  
**Cc:** Lyles, Darrin V. (CMS/OIS); 'Duane.Cummings@cgifederal.com'  
**Subject:** RE: Admin passwords and insecurity in healthcare.gov

Good Morning Tom,

The NotResp team has taken a look at the issue noted in the thread and has passed it along to the NotR<sub>esp</sub> team working on the [www.healthcare.gov](http://www.healthcare.gov) site for OC.

NOTE: I'm not sure if Brian wants to add anything else to this email.

Stacie

**From:** Schankweiler, Thomas W. (CMS/OIS)  
**Sent:** Thursday, October 10, 2013 5:55 PM  
**To:** James, Brian M. (CMS/CCIO)  
**Cc:** Brackett, Stacie D. (CMS/CCIO); Lyles, Darrin V. (CMS/OIS); 'Duane.Cummings@cgifederal.com'  
**Subject:** FW: Admin passwords and insecurity in healthcare.gov  
**Importance:** High

Brian,

I need your contractors to look at this as it relates to the finder page and provide a response by noon Friday. This has attention of the HHS CIO, CMS CIO, and the HHS OIG. An initial response has been provided, but I need your feedback on the Finder page.

[https://www.trustedsec.com/october\\_2013/affordable-health-care-website-secure-probably/](https://www.trustedsec.com/october_2013/affordable-health-care-website-secure-probably/) and take a look at the comments to the post pictured below, on twitter (<https://twitter.com/TrustedSec/statuses/388298092971163648>).

Thanks,

Tom

**From:** Quaintance, Eric (CGI Federal) [<mailto:Eric.Quaintance@cgifederal.com>]  
**Sent:** Thursday, October 10, 2013 3:42 PM  
**To:** Schankweiler, Thomas W. (CMS/OIS)  
**Subject:** RE: Admin passwords and insecurity in healthcare.gov

Hi Tom, one add'l bit of information regarding "CKEditor" as referenced here:  
[https://www.trustedsec.com/october\\_2013/affordable-health-care-website-secure-probably/](https://www.trustedsec.com/october_2013/affordable-health-care-website-secure-probably/)

The URL depicted in the Google search results specifies **finder.healthcare.gov**. **Finder** is not part of our project.

#### Eric Quaintance

Healthcare & Compliance | Application Security | H&CP Security Practice

x27.4654 / 610.842.5094 | Herndon: near rm3041 | Fairfax: 6th West-001A

**From:** Schankweiler, Thomas W. (CMS/OIS) [<mailto:thomas.schankweiler@cms.hhs.gov>]  
**Sent:** Thursday, October 10, 2013 2:14 PM  
**To:** Quaintance, Eric (CGI Federal)  
**Subject:** Fw: Admin passwords and insecurity in healthcare.gov

Fyi

**From:** Schankweiler, Thomas W. (CMS/OIS)  
**Sent:** Thursday, October 10, 2013 02:08 PM  
**To:** Fryer, Teresa M. (CMS/OIS)

**Cc:** Ashbaugh, Jason L. (CMS/OIS); Linares, George E. (CMS/OIS); Outerbridge, Monique (CMS/OIS); Oh, Mark U. (CMS/OIS); Chao, Henry (CMS/OIS); Warren, Kevin (CMS/OIS) ([Kevin.Warren@cms.hhs.gov](mailto:Kevin.Warren@cms.hhs.gov))

**Subject:** RE: Admin passwords and insecurity in healthcare.gov

Hello all,

Here is the feedback regarding this inquiry.

**Statement:**

**CMS [NotRes] p acknowledges the feedback by the security community. Analysis of the code and a review of the operational environment has confirmed that the site is secure and operating with low risk to consumers.**

The code that has been reposted to Pastebin and commented on by TrustedSec is intended to be available to the public code as it makes the user interface (UI) of the site function. By design, these "resource bundles" contain all of the non-personalized text the user will see throughout the site. There is no admin level ID's or passwords located within the [NotRes] [NotRes] posted on-line. The code base at [NotRes] has also just been queried for strings such as "admin password" and "abc123gov" per the twitter screenshot. No evidence was located that there is admin credential revealed. The person who retweeted with the abc password is just being humorous.

The [NotRes] and the SCA test team does run all of the tools mentioned in the article. A lot of commented code was removed prior to production, and the need to perform [NotRes] is a roadmap item, in fact it is scheduled for release to the [NotRes] environment tonight. Performing minification requires a lot of testing to ensure the application is not broken during [NotRes] compression. . As [NotRes] can be improved they will be release with subsequent builds.

To the other points in the article The marketplace does not use PHP so that is a non-issue. The use of Captcha was considered at one time, but removed to ensure 508-Compliance and to more importantly to remove burden on a consumer as *A Good Consumer Experience* was a design consideration. Also the concept of guessing ID's to see if there is a valid one or not is a known risk. We can look into taking steps at locking down access controls further, but it would negatively effect the user-experience.

Regards,

Tom Schankweiler, CISSP  
Information Security Officer, CCIO  
CMS\OIS\CIISG  
Consumer Information and Insurance Systems Group  
410-786-5956 (Balt. Office, N2-13-22)  
[b)(6)] Mobile)

**From:** Charest, Kevin (OS/ASA/OCIO/OIS)

**Sent:** Thursday, October 10, 2013 12:21 PM

**To:** Fryer, Teresa M. (CMS/OIS); Schankweiler, Thomas W. (CMS/OIS)

**Cc:** Baitman, Frank (OS/ASA/OCIO)

**Subject:** FW: Admin passwords and insecurity in healthcare.gov

**Importance:** High

Teresa and Tom,

As you can see from the email chain below and the article at the Trustedsec site there are a significant number of concerns being raised here and they do appear to be legitimate even partially.

I need for you to review the current status of imbedded developer comment and ensure that they are removed. If – as is implied below, the admin password is something as absurd as what is in the tweet it be immediately changed and should be changed regularly in accordance with security standards and best practices.

Please let me know that you received this message and will be looking into for validation and remediation as soon as possible.

Kevin

Kevin Charest Ph.D., CISSP, PMP  
Chief Information Security Officer  
U.S. Department of Health and Human Services

Email: [Kevin.Charest@hhs.gov](mailto:Kevin.Charest@hhs.gov)

NotResp

Ofc. 202-690-5548; Mobile: (b)(6)

*"Driving secure solutions through innovation and sustainable business practices"*

**From:** (b)(6)

**Sent:** Thursday, October 10, 2013 12:12 PM

**To:** Charest, Kevin (OS/ASA/OCIO/OIS)

**Cc:** (b)(6)

(b)(6)

**Subject:** Admin passwords and insecurity in healthcare.gov

**Importance:** High

Kevin,

NotResp



**TrustedSec** @TrustedSec

2h

Is the Affordable Health Care Website Secure? Probably not.  
trustedsec.com/october\_2013/a... #TrustedSec

Collapse

↩ Reply ↻ Retweet ★ Favorite \*\*\* More

**22**

RETWEETS

**3**

FAVORITES

(b)(6)

6:40 AM - 10 Oct 13 · Details

(b)(6)

(b)(6)

comments in tha

45m

NotResp

Details

(b)(6)

Message

**From:** Schankweiler, Thomas W. (CMS/OIS) [redacted] NotResp  
[redacted] NotResp  
on behalf of Schankweiler, Thomas W. (CMS/OIS)  
**Sent:** 10/11/2013 2:05:44 PM  
**To:** Willard, Adam (CMS/CTR) [redacted] NotResp  
[redacted] NotResp  
**CC:** Villar, Manuel (CMS/CTR) [redacted] NotResp  
[redacted] NotResp Warren, Kevin (CMS/OIS)  
[redacted] NotResp  
[redacted] NotResp  
**Subject:** [redacted] NotResp  
**Attachments:** image001.png; image002.png

FYI, please have analyst update ticket.

**From:** Booth, Jon G. (CMS/OC)  
**Sent:** Friday, October 11, 2013 9:48 AM  
**To:** James, Brian M. (CMS/CCIIO); Schankweiler, Thomas W. (CMS/OIS)  
**Cc:** Brackett, Stacie D. (CMS/CCIIO)  
**Subject:** Re: Admin passwords and insecurity in healthcare.gov

We are checking. If the code in question is there (ckeditor), it is not in use and can be deleted. We will keep everyone posted.

**From:** <James>, Brian Sinclair-James BB <brian.james@cms.hhs.gov>  
**Date:** Friday, October 11, 2013 9:44 AM  
**To:** Thomas Schankweiler BB <thomas.schankweiler@cms.hhs.gov>  
**Cc:** Stacie BB <Stacie.Brackett@cms.hhs.gov>, Jon Booth <jon.booth@cms.hhs.gov>  
**Subject:** FW: Admin passwords and insecurity in healthcare.gov

Tom, 3rd hand report is that this code was inherited from CTAC when the site was transitioned. If that was the case, it may not have been operative by the time of the article. I don't know enough about the particular vulnerability to understand if we really had a problem, or if they just stumbled across residual junk that was partitioned off to where it was harmless. I don't recall hearing about that vulnerability from the first SCAs (which I was involved in), but those were 3 years ago. As you probably recall, Craig was the GTO on the CTAC contract. If people push that deeply, you may need to approach him for answers about the original configuration, but I don't think he has to be drug into it at this point.

Brian James, Director  
Issuer Data Collection & Management Division  
Consumer Support Group, CCIIO  
[brian.james@cms.hhs.gov](mailto:brian.james@cms.hhs.gov)

Centers for Medicare and Medicaid Services (CMS)  
Center for Consumer Information and Insurance  
200 Independence Ave, SW  
Room 733H.02  
Washington, DC 20201

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 fullest extent of the law.

---

**From:** Shropshire, Richard (CMS/CCIIO)  
**Sent:** Friday, October 11, 2013 8:05 AM  
**To:** Cummings, Duane (CGI Federal); James, Brian M. (CMS/CCIIO)  
**Subject:** RE: Admin passwords and insecurity in healthcare.gov  
Correct, OC should take care of it. I wanted to be sure we touched all the bases before responding to Tom.

Thanks.

---

Rusty Shropshire | CSG | CCIIO

Ph: 301.492.4238 | BB: (b)(6)

**From:** Cummings, Duane (CGI Federal) [mailto:Duane.Cummings@cgifederal.com]  
**Sent:** Friday, October 11, 2013 7:19 AM  
**To:** Shropshire, Richard (CMS/CCIIO); James, Brian M. (CMS/CCIIO)  
**Subject:** RE: Admin passwords and insecurity in healthcare.gov

Hi Rusty,

That may be a vulnerability that exists in the plan finder site. I forwarded the information to the CGI team that has taken ownership of the site. It looks like something that existed before the transition and the code was just migrated when the site was transitioned from CTAC. Is this something OC would now handle or would your group still manage this risk/issue?

Thanks,

---

Duane Cummings

CGI Federal | 12601 Fair Lakes Circle, Va. 22033

Phone: 703-227-4704 | Email: [duane.cummings@cgifederal.com](mailto:duane.cummings@cgifederal.com)

Website: [www.cgi.com](http://www.cgi.com)

**From:** Shropshire, Richard (CMS/CCIIO) [mailto:richard.shropshire@cms.hhs.gov]  
**Sent:** Thursday, October 10, 2013 10:53 PM  
**To:** Cummings, Duane (CGI Federal); James, Brian M. (CMS/CCIIO)  
**Subject:** RE: Admin passwords and insecurity in healthcare.gov

What about Eric's email below that states the URL depicted is [finder.healthcare.gov](http://finder.healthcare.gov) (I think it's the last screenshot).

Richard "Rusty" Shropshire  
Issuer Data Collection & Management Division  
CCIIO Consumer Support Group  
ph: 301.492.4238 | bb: (b)(6)  
[richard.shropshire@cms.hhs.gov](mailto:richard.shropshire@cms.hhs.gov)

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 fullest extent of the law.

---

**From:** Cummings, Duane (CGI Federal) [mailto:Duane.Cummings@cgifederal.com]  
**Sent:** Thursday, October 10, 2013 7:52 PM



**To:** James, Brian M. (CMS/CCIIO); Shropshire, Richard (CMS/CCIIO)

**Subject:** FW: Admin passwords and insecurity in healthcare.gov

Hi Brian/Rusty,

I am not sure if you already responded to Tom, but the screen shot(s) appear to be of the consumer portal and not anything related to HIOS or the issue portal. I have passed the email along to the FFM/QHP team here at CGI, but not sure if Tom wanted to direct his request to the CMS QHP team.

Thanks,

---

**Duane Cummings**

CGI Federal | 12601 Fair Lakes Circle, Va. 22033

Phone: 703-227-4704 | Email: [duane.cummings@cgifederal.com](mailto:duane.cummings@cgifederal.com)

Website: [www.cgi.com](http://www.cgi.com)

**From:** Schankweiler, Thomas W. (CMS/OIS) [<mailto:thomas.schankweiler@cms.hhs.gov>]

**Sent:** Thursday, October 10, 2013 5:55 PM

**To:** James, Brian M. (CMS/CCIIO)

**Cc:** Brackett, Stacie D. (CMS/CCIIO); Lyles, Darrin V. (CMS/OIS); Cummings, Duane (CGI Federal)

**Subject:** FW: Admin passwords and insecurity in healthcare.gov

**Importance:** High

Brian,

I need your contractors to look at this as it relates to the finder page and provide a response by noon Friday. This has attention of the HHS CIO, CMS CIO, and the HHS OIG. An initial response has been provided, but I need your feedback on the Finder page.

[https://www.trustedsec.com/october\\_2013/affordable-health-care-website-secure-probably/](https://www.trustedsec.com/october_2013/affordable-health-care-website-secure-probably/) and take a look at the comments to the post pictured below, on twitter (<https://twitter.com/TrustedSec/statuses/388298092971163648>).

Thanks,

Tom

**From:** Quaintance, Eric (CGI Federal) [<mailto:Eric.Quaintance@cgifederal.com>]

**Sent:** Thursday, October 10, 2013 3:42 PM

**To:** Schankweiler, Thomas W. (CMS/OIS)

**Subject:** RE: Admin passwords and insecurity in healthcare.gov

Hi Tom, one add'l bit of information regarding "CKEditor" as referenced here:

[https://www.trustedsec.com/october\\_2013/affordable-health-care-website-secure-probably/](https://www.trustedsec.com/october_2013/affordable-health-care-website-secure-probably/)

The URL depicted in the Google search results specifies **finder.healthcare.gov**. **Finder** is not part of our project.

**Eric Quaintance**

Healthcare & Compliance | Application Security | H&CP Security Practice

x27.4654 / 610.842.5094 | Herndon: near rm3041 | Fairfax: 6th West-001A

**From:** Schankweiler, Thomas W. (CMS/OIS) [mailto:thomas.schankweiler@cms.hhs.gov]  
**Sent:** Thursday, October 10, 2013 2:14 PM  
**To:** Quaintance, Eric (CGI Federal)  
**Subject:** Fw: Admin passwords and insecurity in healthcare.gov

Fyi

**From:** Schankweiler, Thomas W. (CMS/OIS)  
**Sent:** Thursday, October 10, 2013 02:08 PM  
**To:** Fryer, Teresa M. (CMS/OIS)  
**Cc:** Ashbaugh, Jason L. (CMS/OIS); Linares, George E. (CMS/OIS); Outerbridge, Monique (CMS/OIS); Oh, Mark U. (CMS/OIS); Chao, Henry (CMS/OIS); Warren, Kevin (CMS/OIS) (Kevin.Warren@cms.hhs.gov)  
**Subject:** RE: Admin passwords and insecurity in healthcare.gov

Hello all,

Here is the feedback regarding this inquiry.

**Statement:**

CMS [NotResp] acknowledges the feedback by the security community. Analysis of the code and a review of the operational environment has confirmed that the site is secure and operating with low risk to consumers.

The code that has been reposted to Pastebin and commented on by TrustedSec is intended to be available to the public code as it makes the user interface (UI) of the site function. By design, these "resource bundles" contain all of the non-personalized text the user will see throughout the site. There is no admin level ID's or passwords located within the [NotRes] posted on-line. The code base at [NotRes] has also just been queried for strings such as "admin password" and "abc123gov" per the twitter screenshot. No evidence was located that there is admin credential revealed. The person who retweeted with the abc password is just being humorous.

The [NotResp] and the SCA test team does run all of the tools mentioned in the article. A lot of commented code was removed prior to production, and the need to perform [NotResp] a roadmap item, in fact it is scheduled for release to the [NotRes] environment tonight. Performing minification requires a lot of testing to ensure the application is not broken during [NotRes] compression. . As j [NotResp] can be improved they will be release with subsequent builds.

To the other points in the article The marketplace does not use PHP so that is a non-issue. The use of Captcha was considered at one time, but removed to ensure 508-Compliance and to more importantly to remove burden on a consumer as *A Good Consumer Experience* was a design consideration. Also the concept of guessing ID's to see if there is a valid one or not is a known risk. We can look into taking steps at locking down access controls further, but it would negatively effect the user-experience.

Regards,

Tom Schankweiler, CISSP  
Information Security Officer, CCIIO  
CMS\OIS\CIISG  
Consumer Information and Insurance Systems Group

410-786-5956 (Balt. Office, N2-13-22)

(b)(6) (Mobile)

**From:** Charest, Kevin (OS/ASA/OCIO/OIS)  
**Sent:** Thursday, October 10, 2013 12:21 PM  
**To:** Fryer, Teresa M. (CMS/OIS); Schankweiler, Thomas W. (CMS/OIS)  
**Cc:** Baitman, Frank (OS/ASA/OCIO)  
**Subject:** FW: Admin passwords and insecurity in healthcare.gov  
**Importance:** High

Teresa and Tom,

As you can see from the email chain below and the article at the Trustedsec site there are a significant number of concerns being raised here and they do appear to be legitimate even partially.

I need for you to review the current status of imbedded developer comment and ensure that they are removed. If -- as is implied below, the admin password is something as absurd as what is in the tweet it be immediately changed and should be changed regularly in accordance with security standards and best practices.

Please let me know that you received this message and will be looking into for validation and remediation as soon as possible.

Kevin

Kevin Charest Ph.D., CISSP, PMP  
Chief Information Security Officer  
U.S. Department of Health and Human Services

Email: [Kevin.Charest@hhs.gov](mailto:Kevin.Charest@hhs.gov)

NotResp

Ofc. 202-690-5548; Mobile: (b)(6)

*"Driving secure solutions through innovation and sustainable business practices"*

**From:** (b)(6)  
**Sent:** Thursday, October 10, 2013 12:12 PM  
**To:** Charest, Kevin (OS/ASA/OCIO/OIS)  
**Cc:** (b)(6)  
(b)(6)  
**Subject:** Admin passwords and insecurity in healthcare.gov  
**Importance:** High

Kevin,

NotResp



**TrustedSec** @TrustedSec

2h

Is the Affordable Health Care Website Secure? Probably not.  
[trustedsec.com/october\\_2013/a...](http://trustedsec.com/october_2013/a...) #TrustedSec

Collapse

↩ Reply ↻ Retweet ★ Favorite \*\*\* More

**22**

RETWEETS

**3**

FAVORITES

(b)(6)

6:40 AM - 10 Oct 13 · Details

(b)(6)

(b)(6)

comments in tha

45m

NotResp

Details

(b)(6)

Message

**From:** Schankweiler, Thomas W. (CMS/OIS); [NotResp]  
[NotResp]  
on behalf of Schankweiler, Thomas W. (CMS/OIS)  
**Sent:** 10/11/2013 1:36:53 PM  
**To:** James, Brian M. (CMS/CCIIO); [NotResp]  
Brackett, Stacie D. (CMS/CCIIO); [NotResp]  
[NotResp]  
**CC:** Lyles, Darrin V. (CMS/OIS); [NotResp]  
[NotResp]; Duane.Cummings@cgifederal.com'  
[Duane.Cummings@cgifederal.com]; Booth, Jon G. (CMS/OC); [NotResp]  
[NotResp]; Patel, Ketan (CMS/OC); [NotResp]  
[NotResp]  
**Subject:** RE: Admin passwords and insecurity in healthcare.gov

Brian, Thanks, for some reason I had it in the back of my mind that finder was connected to [NotResp]

John and Ketan, Could you please review this thread and get back to me by the noon deadline?

Tom

**From:** James, Brian M. (CMS/CCIIO)  
**Sent:** Friday, October 11, 2013 9:35 AM  
**To:** Schankweiler, Thomas W. (CMS/OIS); Brackett, Stacie D. (CMS/CCIIO)  
**Cc:** Lyles, Darrin V. (CMS/OIS); 'Duane.Cummings@cgifederal.com'; Booth, Jon G. (CMS/OC)  
**Subject:** RE: Admin passwords and insecurity in healthcare.gov

Hey Tom, we can have my contractors take a look, but this is the [NotResp] site... not [NotResp] This is owned, managed and run by OC, and I don't really have any insight. The person who needs to be made aware of this is Jon Booth (or whoever is operating as his ISSO). I don't mean to pass the buck, and anyone can correct me, but I'm doubtful we have any influence over this. If there is anything my group can do to assist, let me know. We'll pass along any insights provided by our contractors.

Brian James, Director  
Issuer Data Collection & Management Division  
Consumer Support Group, CCIIO  
[brian.james@cms.hhs.gov](mailto:brian.james@cms.hhs.gov)

Centers for Medicare and Medicaid Services (CMS)  
Center for Consumer Information and Insurance  
200 Independence Ave, SW  
Room 733H.02  
Washington, DC 20201

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 fullest extent of the law.

**From:** Schankweiler, Thomas W. (CMS/OIS)  
**Sent:** Friday, October 11, 2013 8:57 AM  
**To:** Brackett, Stacie D. (CMS/CCIIO); James, Brian M. (CMS/CCIIO)

**Cc:** Lyles, Darrin V. (CMS/OIS); 'Duane.Cummings@cgifederal.com'

**Subject:** RE: Admin passwords and insecurity in healthcare.gov

Thank you Stacie.

**From:** Brackett, Stacie D. (CMS/CCIIO)

**Sent:** Friday, October 11, 2013 8:57 AM

**To:** Schankweiler, Thomas W. (CMS/OIS); James, Brian M. (CMS/CCIIO)

**Cc:** Lyles, Darrin V. (CMS/OIS); 'Duane.Cummings@cgifederal.com'

**Subject:** RE: Admin passwords and insecurity in healthcare.gov

Good Morning Tom,

The **NotResp** team has taken a look at the issue noted in the thread and has passed it along to the **NotR esp** team working on the finder.healthcare.gov site for OC.

NOTE: I'm not sure if Brian wants to add anything else to this email.

Stacie

**From:** Schankweiler, Thomas W. (CMS/OIS)

**Sent:** Thursday, October 10, 2013 5:55 PM

**To:** James, Brian M. (CMS/CCIIO)

**Cc:** Brackett, Stacie D. (CMS/CCIIO); Lyles, Darrin V. (CMS/OIS); 'Duane.Cummings@cgifederal.com'

**Subject:** FW: Admin passwords and insecurity in healthcare.gov

**Importance:** High

Brian,

I need your contractors to look at this as it relates to the finder page and provide a response by noon Friday. This has attention of the HHS CIO, CMS CIO, and the HHS OIG. An initial response has been provided, but I need your feedback on the Finder page.

[https://www.trustedsec.com/october\\_2013/affordable-health-care-website-secure-probably/](https://www.trustedsec.com/october_2013/affordable-health-care-website-secure-probably/) and take a look at the comments to the post pictured below, on twitter (<https://twitter.com/TrustedSec/statuses/388298092971163648>).

Thanks,

Tom

**From:** Quaintance, Eric (CGI Federal) [<mailto:Eric.Quaintance@cgifederal.com>]

**Sent:** Thursday, October 10, 2013 3:42 PM

**To:** Schankweiler, Thomas W. (CMS/OIS)

**Subject:** RE: Admin passwords and insecurity in healthcare.gov

Hi Tom, one add'l bit of information regarding "CKEditor" as referenced here:

[https://www.trustedsec.com/october\\_2013/affordable-health-care-website-secure-probably/](https://www.trustedsec.com/october_2013/affordable-health-care-website-secure-probably/)

The URL depicted in the Google search results specifies **finder.healthcare.gov**. **Finder** is not part of our project.

## Eric Quaintance

Healthcare & Compliance | Application Security | H&CP Security Practice

x27.4654 / 610.842.5094 | Herndon: near rm3041 | Fairfax: 6th West-001A

**From:** Schankweiler, Thomas W. (CMS/OIS) [mailto:thomas.schankweiler@cms.hhs.gov]

**Sent:** Thursday, October 10, 2013 2:14 PM

**To:** Quaintance, Eric (CGI Federal)

**Subject:** Fw: Admin passwords and insecurity in healthcare.gov

Fyi

**From:** Schankweiler, Thomas W. (CMS/OIS)

**Sent:** Thursday, October 10, 2013 02:08 PM

**To:** Fryer, Teresa M. (CMS/OIS)

**Cc:** Ashbaugh, Jason L. (CMS/OIS); Linares, George E. (CMS/OIS); Outerbridge, Monique (CMS/OIS); Oh, Mark U. (CMS/OIS); Chao, Henry (CMS/OIS); Warren, Kevin (CMS/OIS) (Kevin.Warren@cms.hhs.gov)

**Subject:** RE: Admin passwords and insecurity in healthcare.gov

Hello all,

Here is the feedback regarding this inquiry.

### Statement:

CMS [NotResp] acknowledges the feedback by the security community. Analysis of the code and a review of the operational environment has confirmed that the site is secure and operating with low risk to consumers.

The code that has been reposted to Pastebin and commented on by TrustedSec is intended to be available to the public code as it makes the user interface (UI) of the site function. By design, these "resource bundles" contain all of the non-personalized text the user will see throughout the site. There is no admin level ID's or passwords located within the [NotResp] posted on-line. The code base at [NotResp] has also just been queried for strings such as "admin password" and "abc123gov" per the twitter screenshot. No evidence was located that there is admin credential revealed. The person who retweeted with the abc password is just being humorous.

The [NotResp] and the SCA test team does run all of the tools mentioned in the article. A lot of commented code was removed prior to production, and the need to perform [NotResp] is a roadmap item, in fact it is scheduled for release to the [NotResp] environment tonight. Performing minification requires a lot of testing to ensure the application is not broken during [NotResp] compression. . As [NotResp] can be improved they will be release with subsequent builds.

To the other points in the article The marketplace does not use PHP so that is a non-issue. The use of Captcha was considered at one time, but removed to ensure 508-Compliance and to more importantly to remove burden on a consumer as *A Good Consumer Experience* was a design consideration. Also the concept of guessing ID's to see if there is a valid one or not is a known risk. We can look into taking steps at locking down access controls further, but it would negatively effect the user-experience.

Regards,

Tom Schankweiler, CISSP  
Information Security Officer, CCIIO  
CMS\OIS\CIISG  
Consumer Information and Insurance Systems Group  
410-786-5956 (Balt. Office, N2-13-22)  
(b)(6) (Mobile)

**From:** Charest, Kevin (OS/ASA/OCIO/OIS)  
**Sent:** Thursday, October 10, 2013 12:21 PM  
**To:** Fryer, Teresa M. (CMS/OIS); Schankweiler, Thomas W. (CMS/OIS)  
**Cc:** Baitman, Frank (OS/ASA/OCIO)  
**Subject:** FW: Admin passwords and insecurity in healthcare.gov  
**Importance:** High

Teresa and Tom,

As you can see from the email chain below and the article at the Trustedsec site there are a significant number of concerns being raised here and they do appear to be legitimate even partially.

I need for you to review the current status of imbedded developer comment and ensure that they are removed. If – as is implied below, the admin password is something as absurd as what is in the tweet it be immediately changed and should be changed regularly in accordance with security standards and best practices.

Please let me know that you received this message and will be looking into for validation and remediation as soon as possible.

Kevin

Kevin Charest Ph.D., CISSP, PMP  
Chief Information Security Officer  
U.S. Department of Health and Human Services

Email: Kevin.Charest@hhs.gov

NotResp

Ofc. 202-690-5548; Mobile (b)(6)

*“Driving secure solutions through innovation and sustainable business practices”*



**From:** (b)(6)

**Sent:** Thursday, October 10, 2013 12:12 PM

**To:** Charest, Kevin (OS/ASA/OCIO/OIS)

**Cc:** (b)(6) (b)(6)

**Subject:** Admin passwords and insecurity in healthcare.gov

**Importance:** High

Kevin,

NotResp



**TrustedSec** @TrustedSec

2h

Is the Affordable Health Care Website Secure? Probably not.

[trustedsec.com/october\\_2013/a...](http://trustedsec.com/october_2013/a...) #TrustedSec

Collapse

Reply Retweet Favorite More

22

RETWEETS

3

FAVORITES

(b)(6)

6:40 AM - 10 Oct 13 · Details

45m

(b)(6)

(b)(6)

comments in the

NotResp

Details

(b)(6)

Message

**From:** Schankweiler, Thomas W. (CMS/OIS) [NotResp]  
[NotResp]  
on behalf of Schankweiler, Thomas W. (CMS/OIS)  
**Sent:** 10/11/2013 12:57:27 PM  
**To:** Brackett, Stacie D. (CMS/CCIIO) [NotResp]  
[NotResp] James, Brian M. (CMS/CCIIO) [NotResp]  
[NotResp]  
**CC:** Lyles, Darrin V. (CMS/OIS) [NotResp]  
[NotResp] Duane.Cummings@cgifederal.com'  
[Duane.Cummings@cgifederal.com]  
**Subject:** RE: Admin passwords and insecurity in healthcare.gov

Thank you Stacie.

**From:** Brackett, Stacie D. (CMS/CCIIO)  
**Sent:** Friday, October 11, 2013 8:57 AM  
**To:** Schankweiler, Thomas W. (CMS/OIS); James, Brian M. (CMS/CCIIO)  
**Cc:** Lyles, Darrin V. (CMS/OIS); 'Duane.Cummings@cgifederal.com'  
**Subject:** RE: Admin passwords and insecurity in healthcare.gov

Good Morning Tom,

The [NotResp] team has taken a look at the issue noted in the thread and has passed it along to the [NotResp] team working on the finder.healthcare.gov site for OC.

NOTE: I'm not sure if Brian wants to add anything else to this email.

Stacie

**From:** Schankweiler, Thomas W. (CMS/OIS)  
**Sent:** Thursday, October 10, 2013 5:55 PM  
**To:** James, Brian M. (CMS/CCIIO)  
**Cc:** Brackett, Stacie D. (CMS/CCIIO); Lyles, Darrin V. (CMS/OIS); 'Duane.Cummings@cgifederal.com'  
**Subject:** FW: Admin passwords and insecurity in healthcare.gov  
**Importance:** High

Brian,

I need your contractors to look at this as it relates to the finder page and provide a response by noon Friday. This has attention of the HHS CIO, CMS CIO, and the HHS OIG. An initial response has been provided, but I need your feedback on the Finder page.

[https://www.trustedsec.com/october\\_2013/affordable-health-care-website-secure-probably/](https://www.trustedsec.com/october_2013/affordable-health-care-website-secure-probably/) and take a look at the comments to the post pictured below, on twitter (<https://twitter.com/TrustedSec/statuses/388298092971163648>).

Thanks,

Tom

**From:** Quaintance, Eric (CGI Federal) [mailto:Eric.Quaintance@cgifederal.com]  
**Sent:** Thursday, October 10, 2013 3:42 PM  
**To:** Schankweiler, Thomas W. (CMS/OIS)  
**Subject:** RE: Admin passwords and insecurity in healthcare.gov

Hi Tom, one add'l bit of information regarding "CKEditor" as referenced here:  
[https://www.trustedsec.com/october\\_2013/affordable-health-care-website-secure-probably/](https://www.trustedsec.com/october_2013/affordable-health-care-website-secure-probably/)

The URL depicted in the Google search results specifies **finder.healthcare.gov**. **Finder** is not part of our project.

**Eric Quaintance**

Healthcare & Compliance | Application Security | H&CP Security Practice  
x27.4654 / 610.842.5094 | Herndon: near rm3041 | Fairfax: 6th West-001A

**From:** Schankweiler, Thomas W. (CMS/OIS) [mailto:thomas.schankweiler@cms.hhs.gov]  
**Sent:** Thursday, October 10, 2013 2:14 PM  
**To:** Quaintance, Eric (CGI Federal)  
**Subject:** Fw: Admin passwords and insecurity in healthcare.gov

Fyi

**From:** Schankweiler, Thomas W. (CMS/OIS)  
**Sent:** Thursday, October 10, 2013 02:08 PM  
**To:** Fryer, Teresa M. (CMS/OIS)  
**Cc:** Ashbaugh, Jason L. (CMS/OIS); Linares, George E. (CMS/OIS); Outerbridge, Monique (CMS/OIS); Oh, Mark U. (CMS/OIS); Chao, Henry (CMS/OIS); Warren, Kevin (CMS/OIS) (Kevin.Warren@cms.hhs.gov)  
**Subject:** RE: Admin passwords and insecurity in healthcare.gov

Hello all,

Here is the feedback regarding this inquiry.

**Statement:**

**CMS** NotResp acknowledges the feedback by the security community. Analysis of the code and a review of the operational environment has confirmed that the site is secure and operating with low risk to consumers.

The code that has been reposted to Pastebin and commented on by TrustedSec is intended to be available to the public code as it makes the user interface (UI) of the site function. By design, these "resource bundles" contain all of the non-personalized text the user will see throughout the site. There is no admin level ID's or passwords located within the NotResp sp posted on-line. The code base at NotRes has also just been queried for strings such as "admin password" and "abc123gov" per the twitter screenshot. No evidence was located that there is admin credential revealed. The person who retweeted with the abc password is just being humorous.

The NotResp and the SCA test team does run all of the tools mentioned in the article. A lot of commented code was removed prior to production, and the need to perform NotResp is a

roadmap item, in fact it is scheduled for release to the [redacted] sp. environment tonight. Performing minification requires a lot of testing to ensure the application is not broken during [redacted] compression. . As [redacted] can be improved they will be release with subsequent builds.

To the other points in the article The marketplace does not use PHP so that is a non-issue. The use of Captcha was considered at one time, but removed to ensure 508-Compliance and to more importantly to remove burden on a consumer as *A Good Consumer Experience* was a design consideration. Also the concept of guessing ID's to see if there is a valid one or not is a known risk. We can look into taking steps at locking down access controls further, but it would negatively effect the user-experience.

Regards,

Tom Schankweiler, CISSP  
Information Security Officer, CCIIO  
CMS\OIS\CIISG  
Consumer Information and Insurance Systems Group  
410-786-5956 (Balt. Office, N2-13-22)  
[redacted] (b)(6) (Mobile)

**From:** Charest, Kevin (OS/ASA/OCIO/OIS)  
**Sent:** Thursday, October 10, 2013 12:21 PM  
**To:** Fryer, Teresa M. (CMS/OIS); Schankweiler, Thomas W. (CMS/OIS)  
**Cc:** Baitman, Frank (OS/ASA/OCIO)  
**Subject:** FW: Admin passwords and insecurity in healthcare.gov  
**Importance:** High

Teresa and Tom,

As you can see from the email chain below and the article at the Trustedsec site there are a significant number of concerns being raised here and they do appear to be legitimate even partially.

I need for you to review the current status of imbedded developer comment and ensure that they are removed. If – as is implied below, the admin password is something as absurd as what is in the tweet it be immediately changed and should be changed regularly in accordance with security standards and best practices.

Please let me know that you received this message and will be looking into for validation and remediation as soon as possible.

Kevin

Kevin Charest Ph.D., CISSP, PMP  
Chief Information Security Officer  
U.S. Department of Health and Human Services

Email: [Kevin.Charest@hhs.gov](mailto:Kevin.Charest@hhs.gov)

NotResp

Ofc. 202-690-5548; Mobile (b)(6)

*"Driving secure solutions through innovation and sustainable business practices"*

**From:** (b)(6)

**Sent:** Thursday, October 10, 2013 12:12 PM

**To:** Charest, Kevin (OS/ASA/OCIO/OIS)

**Cc:** (b)(6)

(b)(6)

**Subject:** Admin passwords and insecurity in healthcare.gov

**Importance:** High

Kevin,

NotResp



**TrustedSec** @TrustedSec

2h

Is the Affordable Health Care Website Secure? Probably not.

[trustedsec.com/october\\_2013/a...](http://trustedsec.com/october_2013/a...) #TrustedSec

Collapse

Reply Retweet Favorite More

**22**

RETWEETS

**3**

FAVORITES

(b)(6)

6:40 AM - 10 Oct 13 · Details

45m

(b)(6)

(b)(6)

comments in tha

NotResp

Details

(b)(6)

(b)(6)

Message

**From:** Schankweiler, Thomas W. (CMS/OIS) [NotResp]  
**Sent:** 10/10/2013 6:14:00 PM [NotResp]  
**To:** 'Eric.Quaintance@cgifederal.com' [Eric.Quaintance@cgifederal.com]  
**Subject:** Fw: Admin passwords and insecurity in healthcare.gov

Fyi

**From:** Schankweiler, Thomas W. (CMS/OIS)  
**Sent:** Thursday, October 10, 2013 02:08 PM  
**To:** Fryer, Teresa M. (CMS/OIS)  
**Cc:** Ashbaugh, Jason L. (CMS/OIS); Linares, George E. (CMS/OIS); Outerbridge, Monique (CMS/OIS); Oh, Mark U. (CMS/OIS); Chao, Henry (CMS/OIS); Warren, Kevin (CMS/OIS) (Kevin.Warren@cms.hhs.gov)  
**Subject:** RE: Admin passwords and insecurity in healthcare.gov

Hello all,

Here is the feedback regarding this inquiry.

**Statement:**

CMS [NotResp] acknowledges the feedback by the security community. Analysis of the code and a review of the operational environment has confirmed that the site is secure and operating with low risk to consumers.

The code that has been reposted to Pastebin and commented on by TrustedSec is intended to be available to the public code as it makes the user interface (UI) of the site function. By design, these "resource bundles" contain all of the non-personalized text the user will see throughout the site. There is no admin level ID's or passwords located within the [NotResp] posted on-line. The code base at [NotResp] has also just been queried for strings such as "admin password" and "abc123gov" per the twitter screenshot. No evidence was located that there is admin credential revealed. The person who retweeted with the abc password is just being humorous.

The [NotResp] and the SCA test team does run all of the tools mentioned in the article. A lot of commented code was removed prior to production, and the need to perform [NotResp] is a roadmap item, in fact it is scheduled for release to the [NotResp] environment tonight. Performing minification requires a lot of testing to ensure the application is not broken during [NotResp] compression. As [NotResp] can be improved they will be release with subsequent builds.

To the other points in the article The marketplace does not use PHP so that is a non-issue. The use of Captcha was considered at one time, but removed to ensure 508-Compliance and to more importantly to remove burden on a consumer as *A Good Consumer Experience* was a design consideration. Also the concept of guessing ID's to see if there is a valid one or not is a known risk. We can look into taking steps at locking down access controls further, but it would negatively effect the user-experience.

Regards,

Tom Schankweiler, CISSP  
 Information Security Officer, CCIIO

CMS\OIS\CIISG

Consumer Information and Insurance Systems Group

410-786-5956 (Balt. Office, N2-13-22)

(b)(6) (Mobile)

**From:** Charest, Kevin (OS/ASA/OCIO/OIS)

**Sent:** Thursday, October 10, 2013 12:21 PM

**To:** Fryer, Teresa M. (CMS/OIS); Schankweiler, Thomas W. (CMS/OIS)

**Cc:** Baitman, Frank (OS/ASA/OCIO)

**Subject:** FW: Admin passwords and insecurity in healthcare.gov

**Importance:** High

Teresa and Tom,

As you can see from the email chain below and the article at the Trustedsec site there are a significant number of concerns being raised here and they do appear to be legitimate even partially.

I need for you to review the current status of imbedded developer comment and ensure that they are removed. If – as is implied below, the admin password is something as absurd as what is in the tweet it be immediately changed and should be changed regularly in accordance with security standards and best practices.

Please let me know that you received this message and will be looking into for validation and remediation as soon as possible.

Kevin

Kevin Charest Ph.D., CISSP, PMP

Chief Information Security Officer

U.S. Department of Health and Human Services

Email: Kevin.Charest@hhs.gov

NotResp

Ofc. 202-690-5548; Mobile: (b)(6)

*“Driving secure solutions through innovation and sustainable business practices”*

**From:** (b)(6)

**Sent:** Thursday, October 10, 2013 12:12 PM

**To:** Charest, Kevin (OS/ASA/OCIO/OIS)

**Cc:** (b)(6)

(b)(6)



**Subject:** Admin passwords and insecurity in healthcare.gov

**Importance:** High

Kevin,

NotResp



**TrustedSec** @TrustedSec

2h

Is the Affordable Health Care Website Secure? Probably not.

[trustedsec.com/october\\_2013/a...](http://trustedsec.com/october_2013/a...) #TrustedSec

Collapse

Reply Retweet Favorite More

**22**

RETWEETS

**3**

FAVORITES

(b)(6)

6:40 AM - 10 Oct 13 · Details

(b)(6)

(b)(6)

comments in tha

45m

(b)(6)

Details

(b)(6)

Message

**From:** Schankweiler, Thomas W. (CMS/OIS) [NotResp]  
[NotResp]  
**Sent:** 10/10/2013 6:16:09 PM  
**To:** Ashbaugh, Jason L. (CMS/OIS) [NotResp]  
**Subject:** Re: Admin passwords and insecurity in healthcare.gov

Concur with assessment.

**From:** Ashbaugh, Jason L. (CMS/OIS)  
**Sent:** Thursday, October 10, 2013 02:15 PM  
**To:** Schankweiler, Thomas W. (CMS/OIS)  
**Subject:** RE: Admin passwords and insecurity in healthcare.gov

One thing to consider from the google search that found .php

That could be an older artifact from the earlier version of healthcare.gov before it was relaunched as well. I don't see any indication that it's a live link, or even a valid uri path.

Thanks,

Jason L. Ashbaugh  
CMS Computer Security Incident Response (CSIRT) - Lead  
Enterprise Information Security Group (EISG)  
Centers for Medicare & Medicaid Services  
(w) 410.786.3017  
(bb) [Redacted]

---

**From:** Schankweiler, Thomas W. (CMS/OIS)  
**Sent:** Thursday, October 10, 2013 2:08 PM  
**To:** Fryer, Teresa M. (CMS/OIS)  
**Cc:** Ashbaugh, Jason L. (CMS/OIS); Linares, George E. (CMS/OIS); Outerbridge, Monique (CMS/OIS); Oh, Mark U. (CMS/OIS); Chao, Henry (CMS/OIS); Warren, Kevin (CMS/OIS)  
**Subject:** RE: Admin passwords and insecurity in healthcare.gov  
Hello all,

Here is the feedback regarding this inquiry.

**Statement:**

**CMS [Redacted] acknowledges the feedback by the security community. Analysis of the code and a review of the operational environment has confirmed that the site is secure and operating with low risk to consumers.**

The code that has been reposted to Pastebin and commented on by TrustedSec is intended to be available to the public code as it makes the user interface (UI) of the site function. By design, these "resource bundles" contain all of the non-personalized text the user will see throughout the site. There is no admin level ID's or passwords located within the [Redacted] posted on-line. The code base at [Redacted] has also just been queried for strings such as "admin password" and [Redacted]

"abc123gov" per the twitter screenshot. No evidence was located that there is admin credential revealed. The person who retweeted with the abc password is just being humorous.

The [NotResp] and the SCA test team does run all of the tools mentioned in the article. A lot of commented code was removed prior to production, and the need to perform [NotResp] is a roadmap item, in fact it is scheduled for release to the [NotRes] environment tonight. Performing minification requires a lot of testing to ensure the application is not broken during [NotRes] compression. . As [NotResp] can be improved they will be release with subsequent builds.

To the other points in the article The marketplace does not use PHP so that is a non-issue. The use of Captcha was considered at one time, but removed to ensure 508-Compliance and to more importantly to remove burden on a consumer as *A Good Consumer Experience* was a design consideration. Also the concept of guessing ID's to see if there is a valid one or not is a known risk. We can look into taking steps at locking down access controls further, but it would negatively effect the user-experience.

Regards,

Tom Schankweiler, CISSP  
Information Security Officer, CCIO  
CMS\OIS\CIISG  
Consumer Information and Insurance Systems Group  
410-786-5956 (Balt. Office, N2-13-22)  
[b)(6)] (Mobile)

**From:** Charest, Kevin (OS/ASA/OCIO/OIS)  
**Sent:** Thursday, October 10, 2013 12:21 PM  
**To:** Fryer, Teresa M. (CMS/OIS); Schankweiler, Thomas W. (CMS/OIS)  
**Cc:** Baitman, Frank (OS/ASA/OCIO)  
**Subject:** FW: Admin passwords and insecurity in healthcare.gov  
**Importance:** High

Teresa and Tom,

As you can see from the email chain below and the article at the Trustedsec site there are a significant number of concerns being raised here and they do appear to be legitimate even partially.

I need for you to review the current status of imbedded developer comment and ensure that they are removed. If – as is implied below, the admin password is something as absurd as what is in the tweet it be immediately changed and should be changed regularly in accordance with security standards and best practices.

Please let me know that you received this message and will be looking into for validation and remediation as soon as possible.

Kevin

Kevin Charest Ph.D., CISSP, PMP  
Chief Information Security Officer  
U.S. Department of Health and Human Services

Email: [Kevin.Charest@hhs.gov](mailto:Kevin.Charest@hhs.gov)

NotResp

Ofc. 202-690-5548; Mobile: (b)(6)

*"Driving secure solutions through innovation and sustainable business practices"*

**From:** (b)(6)

**Sent:** Thursday, October 10, 2013 12:12 PM

**To:** Charest, Kevin (OS/ASA/OCIO/OIS)

**Cc:** (b)(6)

(b)(6)

**Subject:** Admin passwords and insecurity in healthcare.gov

**Importance:** High

Kevin,

NotResp



**TrustedSec** @TrustedSec

2h

Is the Affordable Health Care Website Secure? Probably not.

[trustedsec.com/october\\_2013/a...](http://trustedsec.com/october_2013/a...) #TrustedSec

Collapse

Reply Retweet Favorite More

22

RETWEETS

3

FAVORITES

(b)(6)

6:40 AM - 10 Oct 13 · Details

(b)(6)	(b)(6)	comments in tha
	NotResp	

45m

Details

(b)(6)

Message

**From:** Schankweiler, Thomas W. (CMS/OIS) [NotResp]  
 [NotResp]  
 on behalf of Schankweiler, Thomas W. (CMS/OIS)  
**Sent:** 11/3/2013 8:51:12 PM  
**To:** Outerbridge, Monique (CMS/OIS) [NotResp]  
 [NotResp] Nelson, David J. [NotResp]  
 [NotResp] Bradley, Tasha (CMS/OC) [NotResp]  
 [NotResp] Grothe, Kirk A. (CMS/OIS) [NotResp]  
 [NotResp]; Oh, Mark U.  
 (CMS/OIS) [NotResp]  
 'greg.gershman.health@gmail.com' [greg.gershman.health@gmail.com]  
**CC:** Unruh, Patti (CMS/OC) [NotResp]  
**Subject:** RE: question from CNN about Heritage report

I read this e-mail just within the last hour. I need to read the new article. Was CGI able to duplicate this problem? I am assuming so since they are putting a fix in place.

Tom

**From:** Outerbridge, Monique (CMS/OIS)  
**Sent:** Sunday, November 03, 2013 3:50 PM  
**To:** Nelson, David J. (CMS/OEM); Bradley, Tasha (CMS/OC); Grothe, Kirk A. (CMS/OIS); Oh, Mark U. (CMS/OIS); Schankweiler, Thomas W. (CMS/OIS); 'greg.gershman.health@gmail.com'  
**Cc:** Unruh, Patti (CMS/OC)  
**Subject:** RE: question from CNN about Heritage report

CGI just informed us of this problem this afternoon. They are working on a fix now and could be deployed to production in 2 hours. Will keep you posted.

---

**From:** Nelson, David J. (CMS/OEM)  
**Sent:** Sunday, November 03, 2013 3:48 PM  
**To:** Bradley, Tasha (CMS/OC); Outerbridge, Monique (CMS/OIS); Grothe, Kirk A. (CMS/OIS); Oh, Mark U. (CMS/OIS); Schankweiler, Thomas W. (CMS/OIS); 'greg.gershman.health@gmail.com'  
**Cc:** Unruh, Patti (CMS/OC)  
**Subject:** RE: question from CNN about Heritage report

I am just hearing about this following your note. I am hoping Tom is in the loop.

**From:** Bradley, Tasha (CMS/OC)  
**Sent:** Sunday, November 03, 2013 3:02 PM  
**To:** Nelson, David J. (CMS/OEM); Outerbridge, Monique (CMS/OIS); Grothe, Kirk A. (CMS/OIS); Oh, Mark U. (CMS/OIS); Schankweiler, Thomas W. (CMS/OIS); 'greg.gershman.health@gmail.com'  
**Cc:** Unruh, Patti (CMS/OC)  
**Subject:** Fw: question from CNN about Heritage report

Hi all- sorry for the Sunday afternoon email. CNN is working on a story based on a Heritage report that a user received another user's eligibility determination.

Is this possible?

If this does happen, what is the procedure to address this?

Are there security measures in place to handle a situation like this?

Is the team aware of any instances that this has occurred?

<http://blog.heritage.org/2013/11/02/exclusive-healthcare-gov-users-warn-of-security-risk-breach-of-privacy/>

**From:** Bataille, Julie (CMS/OC)

**Sent:** Sunday, November 03, 2013 02:22 PM

**To:** Bradley, Tasha (CMS/OC)

**Subject:** Fw: question from CNN about Heritage report

Can u pls take

**From:** Wallace, Gregory [<mailto:gregory.wallace@turner.com>]

**Sent:** Sunday, November 03, 2013 02:16 PM

**To:** Bataille, Julie (CMS/OC); Cook, Brian T. (CMS/OC)

**Subject:** question from CNN about Heritage report

Good afternoon,

Checking in for your comment on this Heritage post that a user's information was presented to a different user on HealthCare.gov.

Is this an issue CMS teams are aware of and working on, and are there other instances of this happening?

<http://blog.heritage.org/2013/11/02/exclusive-healthcare-gov-users-warn-of-security-risk-breach-of-privacy/>

Thank you,

Greg Wallace

CNN

202-738-3113

Message

**From:** Schankweiler, Thomas W. (CMS/OIS) [NotResp]  
[NotResp]  
on behalf of Schankweiler, Thomas W. (CMS/OIS)  
**Sent:** 10/14/2013 11:50:49 AM  
**To:** 'Quaintance, Eric (CGI Federal)' [Eric.Quaintance@cgifederal.com]  
**CC:** Desai, Rupak (CGI Federal) [Rupak.Desai@cgifederal.com]; Goodrich, Lynn F (CGI Federal) [lynn.goodrich@cgifederal.com]; Hewitt, James (CGI Federal) [James.Hewitt@cgifederal.com]; Ramamoorthy, Balaji Manikandan (CGI Federal) [balajimanikandan.ramamoorthy@cgifederal.com]  
**Subject:** RE: Admin passwords and insecurity in healthcare.gov

Eric,

Understood [NotResp] has been looking into this issue and is preparing to resolve it.

Thank you,

Tom

**From:** Quaintance, Eric (CGI Federal) [mailto:Eric.Quaintance@cgifederal.com]  
**Sent:** Sunday, October 13, 2013 2:04 AM  
**To:** Schankweiler, Thomas W. (CMS/OIS)  
**Cc:** Desai, Rupak (CGI Federal); Goodrich, Lynn F (CGI Federal); Hewitt, James (CGI Federal); Ramamoorthy, Balaji Manikandan (CGI Federal)  
**Subject:** RE: Admin passwords and insecurity in healthcare.gov

Good morning Tom,

This update is in reference to the questionable [NotResp] item recently identified by [NotResp]

Our CMS Websites group (CWS) has indicated [NotResp] has not yet taken ownership of the [NotResp] healthcare.gov applications. The production site is currently hosted in the CMS cloud and allegedly owned by OIS. Although CWS is currently re-skinning and redesigning the site, it is not slated to go live until November.

CWS has raised the issue with [NotResp] In the meantime, please reach out if we can assist further.

**Eric Quaintance**

**CGI FEDERAL**

12601 Fair Lakes Circle, 6W-001  
Fairfax, VA 22030 | 703.227.4654

**From:** Schankweiler, Thomas W. (CMS/OIS) [mailto:thomas.schankweiler@cms.hhs.gov]  
**Sent:** Thursday, October 10, 2013 2:14 PM  
**To:** Quaintance, Eric (CGI Federal)  
**Subject:** Fw: Admin passwords and insecurity in healthcare.gov

Fyi



**From:** Schankweiler, Thomas W. (CMS/OIS)

**Sent:** Thursday, October 10, 2013 02:08 PM

**To:** Fryer, Teresa M. (CMS/OIS)

**Cc:** Ashbaugh, Jason L. (CMS/OIS); Linares, George E. (CMS/OIS); Outerbridge, Monique (CMS/OIS); Oh, Mark U. (CMS/OIS); Chao, Henry (CMS/OIS); Warren, Kevin (CMS/OIS) ([Kevin.Warren@cms.hhs.gov](mailto:Kevin.Warren@cms.hhs.gov))

**Subject:** RE: Admin passwords and insecurity in healthcare.gov

Hello all,

Here is the feedback regarding this inquiry.

**Statement:**

CMS NotResp acknowledges the feedback by the security community. Analysis of the code and a review of the operational environment has confirmed that the site is secure and operating with low risk to consumers.

The code that has been reposted to Pastebin and commented on by TrustedSec is intended to be available to the public code as it makes the user interface (UI) of the site function. By design, these "resource bundles" contain all of the non-personalized text the user will see throughout the site. There is no admin level ID's or passwords located within the NotRes posted on-line. The code base at NotRes has also just been queried for strings such as "admin password" and "abc123gov" per the twitter screenshot. No evidence was located that there is admin credential revealed. The person who retweeted with the abc password is just being humorous.

The NotResp team and the SCA test team does run all of the tools mentioned in the article. A lot of commented code was removed prior to production, and the need to perform NotResp is a roadmap item, in fact it is scheduled for release to the NotRes environment tonight. Performing minimization requires a lot of testing to ensure the application is not broken during NotRes compression. As NotResp can be improved they will be release with subsequent builds.

To the other points in the article The marketplace does not use PHP so that is a non-issue. The use of Captcha was considered at one time, but removed to ensure 508-Compliance and to more importantly to remove burden on a consumer as *A Good Consumer Experience* was a design consideration. Also the concept of guessing ID's to see if there is a valid one or not is a known risk. We can look into taking steps at locking down access controls further, but it would negatively effect the user-experience.

Regards,

Tom Schankweiler, CISSP

Information Security Officer, CCIO

CMS\OIS\CIISG

Consumer Information and Insurance Systems Group

410-786-5956 (Balt. Office, N2-13-22)

(b)(6) (Mobile)

**From:** Charest, Kevin (OS/ASA/OCIO/OIS)  
**Sent:** Thursday, October 10, 2013 12:21 PM  
**To:** Fryer, Teresa M. (CMS/OIS); Schankweiler, Thomas W. (CMS/OIS)  
**Cc:** Baitman, Frank (OS/ASA/OCIO)  
**Subject:** FW: Admin passwords and insecurity in healthcare.gov  
**Importance:** High

Teresa and Tom,

As you can see from the email chain below and the article at the Trustedsec site there are a significant number of concerns being raised here and they do appear to be legitimate even partially.

I need for you to review the current status of imbedded developer comment and ensure that they are removed. If -- as is implied below, the admin password is something as absurd as what is in the tweet it be immediately changed and should be changed regularly in accordance with security standards and best practices.

Please let me know that you received this message and will be looking into for validation and remediation as soon as possible.

Kevin

Kevin Charest Ph.D., CISSP, PMP  
Chief Information Security Officer  
U.S. Department of Health and Human Services

Email: Kevin.Charest@hhs.gov

NotResp

Ofc. 202-690-5548; Mobile

(b)(6)

*"Driving secure solutions through innovation and sustainable business practices"*

**From:** (b)(6)

**Sent:** Thursday, October 10, 2013 12:12 PM

**To:** Charest, Kevin (OS/ASA/OCIO/OIS)

**Cc:** (b)(6)

(b)(6)

**Subject:** Admin passwords and insecurity in healthcare.gov

**Importance:** High

Kevin,

NotResp



**TrustedSec** @TrustedSec

2h

Is the Affordable Health Care Website Secure? Probably not.

trustedsec.com/october\_2013/a... #TrustedSec

Collapse

Reply Retweet Favorite More

**22**

RETWEETS

**3**

FAVORITES

(b)(6)

6:40 AM - 10 Oct 13 · Details

45m

(b)(6)

(b)(6)

comments in tha

NotResp

Details

(b)(6)

Message

**From:** Schankweiler, Thomas W. (CMS/OIS) [NotResp]  
 [NotResp]  
 on behalf of Schankweiler, Thomas W. (CMS/OIS)  
**Sent:** 10/11/2013 2:05:11 PM  
**To:** Willard, Adam (CMS/CTR) [NotResp]  
 [NotResp]  
**CC:** Orlando, Mark (CMS/CTR) [NotResp]  
 [NotResp] Warren, Kevin (CMS/OIS)  
 [NotResp]  
 [NotResp]  
**Subject:** FW: Admin passwords and insecurity in healthcare.gov

FYI... please have the analyst update ticket.

**From:** Patel, Ketan (CMS/OC)  
**Sent:** Friday, October 11, 2013 9:59 AM  
**To:** Schankweiler, Thomas W. (CMS/OIS); James, Brian M. (CMS/CCIIO); Brackett, Stacie D. (CMS/CCIIO)  
**Cc:** Lyles, Darrin V. (CMS/OIS); 'Duane.Cummings@cgifederal.com'; Booth, Jon G. (CMS/OC)  
**Subject:** RE: Admin passwords and insecurity in healthcare.gov

Since we get 404 we do not have that page there. Other approach is we can make request to Google to drop of it from their index.

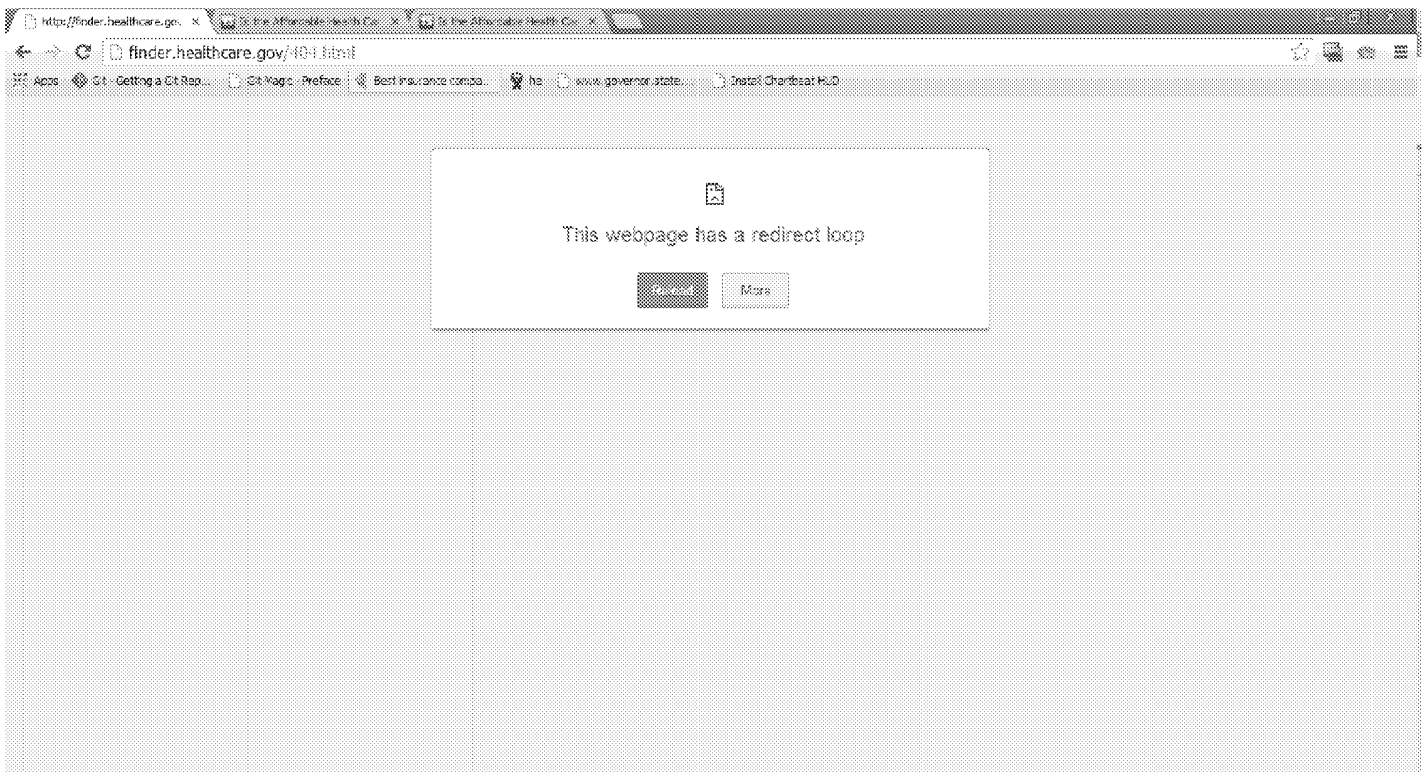
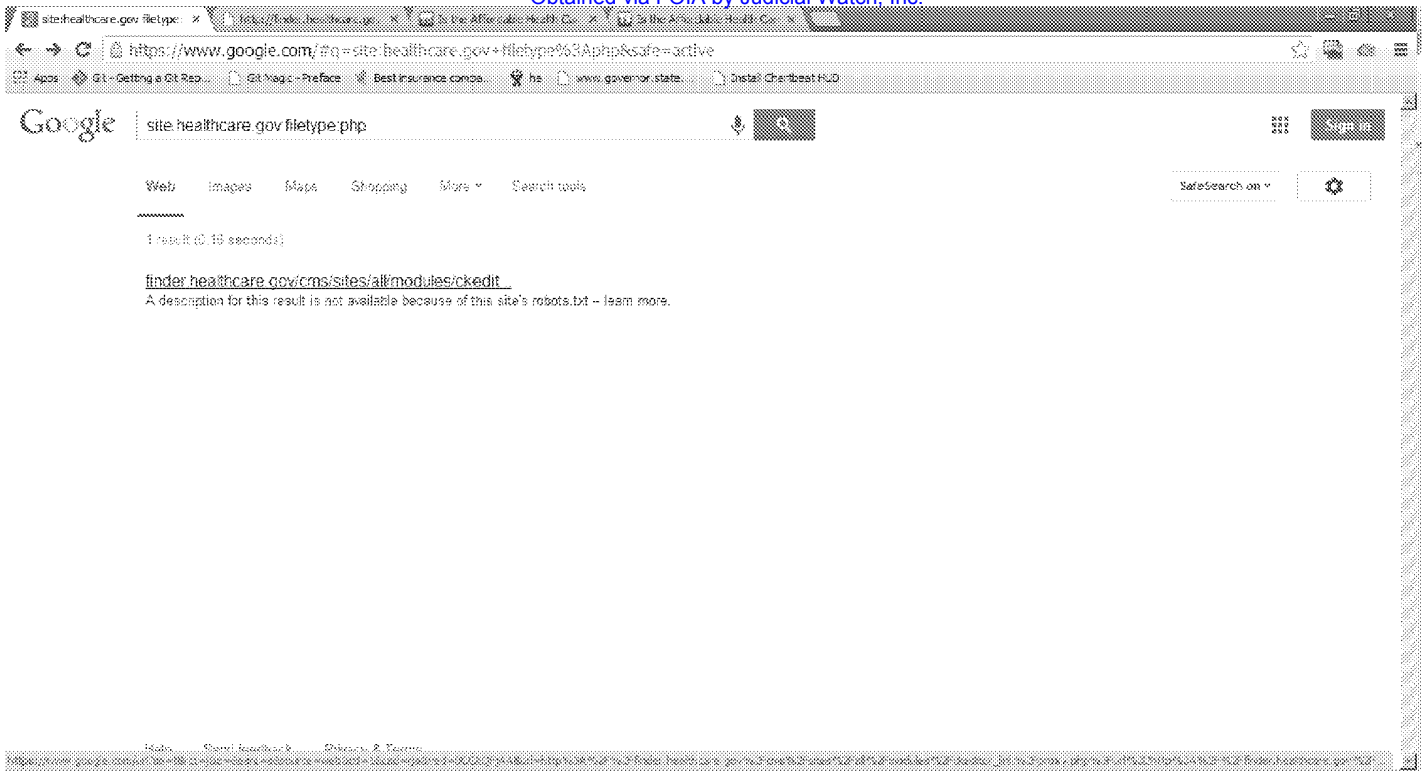
**From:** Schankweiler, Thomas W. (CMS/OIS)  
**Sent:** Friday, October 11, 2013 9:56 AM  
**To:** Patel, Ketan (CMS/OC); James, Brian M. (CMS/CCIIO); Brackett, Stacie D. (CMS/CCIIO)  
**Cc:** Lyles, Darrin V. (CMS/OIS); 'Duane.Cummings@cgifederal.com'; Booth, Jon G. (CMS/OC)  
**Subject:** RE: Admin passwords and insecurity in healthcare.gov

Yeah we saw the same thing. Should the page just be pulled down?

**From:** Patel, Ketan (CMS/OC)  
**Sent:** Friday, October 11, 2013 9:53 AM  
**To:** Schankweiler, Thomas W. (CMS/OIS); James, Brian M. (CMS/CCIIO); Brackett, Stacie D. (CMS/CCIIO)  
**Cc:** Lyles, Darrin V. (CMS/OIS); 'Duane.Cummings@cgifederal.com'; Booth, Jon G. (CMS/OC)  
**Subject:** RE: Admin passwords and insecurity in healthcare.gov

Tom,  
 Finder.Healthcare.gov was as is migration from department we have done no development on existing Finder Applications. Codebase with no detailed documentation was given to us by HHS. Current Finder application was configured with help from Peter. I just tried below and the  
 clicked [https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&ved=0CCkQFjAA&url=http%3A%2F%2Ffinder.healthcare.gov%2Fcms%2Fsites%2Fall%2Fmodules%2Fckeditor\\_link%2Fproxy.php%3Furl%3Dhttp%3A%2F%2Ffinder.healthcare.gov%2F&ei=GwBYUpS2GJax4AOE94DYAg&usg=AFQjCNGJDAIclz6MGGZu-pexZkSMfg-dsw](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&ved=0CCkQFjAA&url=http%3A%2F%2Ffinder.healthcare.gov%2Fcms%2Fsites%2Fall%2Fmodules%2Fckeditor_link%2Fproxy.php%3Furl%3Dhttp%3A%2F%2Ffinder.healthcare.gov%2F&ei=GwBYUpS2GJax4AOE94DYAg&usg=AFQjCNGJDAIclz6MGGZu-pexZkSMfg-dsw)

I get 404 page.



**From:** Schankweiler, Thomas W. (CMS/OIS)

**Sent:** Friday, October 11, 2013 9:37 AM

**To:** James, Brian M. (CMS/CCIIO); Brackett, Stacie D. (CMS/CCIIO)

**Cc:** Lyles, Darrin V. (CMS/OIS); 'Duane.Cummings@cgifederal.com'; Booth, Jon G. (CMS/OC); Patel, Ketan (CMS/OC)

**Subject:** RE: Admin passwords and insecurity in healthcare.gov

Brian, Thanks, for some reason I had it in the back of my mind that finder was connected to NotRes  
p

John and Ketan, Could you please review this thread and get back to me by the noon deadline?

Tom

**From:** James, Brian M. (CMS/CCIIO)  
**Sent:** Friday, October 11, 2013 9:35 AM  
**To:** Schankweiler, Thomas W. (CMS/OIS); Brackett, Stacie D. (CMS/CCIIO)  
**Cc:** Lyles, Darrin V. (CMS/OIS); 'Duane.Cummings@cgifederal.com'; Booth, Jon G. (CMS/OC)  
**Subject:** RE: Admin passwords and insecurity in healthcare.gov

Hey Tom, we can have my contractors take a look, but this is the PlanFinder site... not NotRe  
sp This is owned, managed and run by OC, and I don't really have any insight. The person who needs to be made aware of this is Jon Booth (or whoever is operating as his ISSO). I don't mean to pass the buck, and anyone can correct me, but I'm doubtful we have any influence over this. If there is anything my group can do to assist, let me know. We'll pass along any insights provided by our contractors.

Brian James, Director  
Issuer Data Collection & Management Division  
Consumer Support Group, CCIIO  
[brian.james@cms.hhs.gov](mailto:brian.james@cms.hhs.gov)

Centers for Medicare and Medicaid Services (CMS)  
Center for Consumer Information and Insurance  
200 Independence Ave, SW  
Room 733H.02  
Washington, DC 20201

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 fullest extent of the law.

---

**From:** Schankweiler, Thomas W. (CMS/OIS)  
**Sent:** Friday, October 11, 2013 8:57 AM  
**To:** Brackett, Stacie D. (CMS/CCIIO); James, Brian M. (CMS/CCIIO)  
**Cc:** Lyles, Darrin V. (CMS/OIS); 'Duane.Cummings@cgifederal.com'  
**Subject:** RE: Admin passwords and insecurity in healthcare.gov  
Thank you Stacie.

**From:** Brackett, Stacie D. (CMS/CCIIO)  
**Sent:** Friday, October 11, 2013 8:57 AM  
**To:** Schankweiler, Thomas W. (CMS/OIS); James, Brian M. (CMS/CCIIO)  
**Cc:** Lyles, Darrin V. (CMS/OIS); 'Duane.Cummings@cgifederal.com'  
**Subject:** RE: Admin passwords and insecurity in healthcare.gov

Good Morning Tom,

The NotResp team has taken a look at the issue noted in the thread and has passed it along to the NOT  
Res team working on the finder.healthcare.gov site for OC.

NOTE: I'm not sure if Brian wants to add anything else to this email.

Stacie

**From:** Schankweiler, Thomas W. (CMS/OIS)  
**Sent:** Thursday, October 10, 2013 5:55 PM  
**To:** James, Brian M. (CMS/CCIO)  
**Cc:** Brackett, Stacie D. (CMS/CCIO); Lyles, Darrin V. (CMS/OIS); 'Duane.Cummings@cgifederal.com'  
**Subject:** FW: Admin passwords and insecurity in healthcare.gov  
**Importance:** High

Brian,

I need your contractors to look at this as it relates to the finder page and provide a response by noon Friday. This has attention of the HHS CIO, CMS CIO, and the HHS OIG. An initial response has been provided, but I need your feedback on the Finder page.

[https://www.trustedsec.com/october\\_2013/affordable-health-care-website-secure-probably/](https://www.trustedsec.com/october_2013/affordable-health-care-website-secure-probably/) and take a look at the comments to the post pictured below, on twitter (<https://twitter.com/TrustedSec/statuses/388298092971163648>).

Thanks,

Tom

**From:** Quaintance, Eric (CGI Federal) [<mailto:Eric.Quaintance@cgifederal.com>]  
**Sent:** Thursday, October 10, 2013 3:42 PM  
**To:** Schankweiler, Thomas W. (CMS/OIS)  
**Subject:** RE: Admin passwords and insecurity in healthcare.gov

Hi Tom, one add'l bit of information regarding "CKEditor" as referenced here:  
[https://www.trustedsec.com/october\\_2013/affordable-health-care-website-secure-probably/](https://www.trustedsec.com/october_2013/affordable-health-care-website-secure-probably/)

The URL depicted in the Google search results specifies **finder.healthcare.gov**. **Finder** is not part of our project.

#### Eric Quaintance

Healthcare & Compliance | Application Security | H&CP Security Practice

x27.4654 / 610.842.5094 | Herndon: near rm3041 | Fairfax: 6th West-001A

**From:** Schankweiler, Thomas W. (CMS/OIS) [<mailto:thomas.schankweiler@cms.hhs.gov>]  
**Sent:** Thursday, October 10, 2013 2:14 PM  
**To:** Quaintance, Eric (CGI Federal)  
**Subject:** Fw: Admin passwords and insecurity in healthcare.gov

Fyi

**From:** Schankweiler, Thomas W. (CMS/OIS)  
**Sent:** Thursday, October 10, 2013 02:08 PM  
**To:** Fryer, Teresa M. (CMS/OIS)



**Cc:** Ashbaugh, Jason L. (CMS/OIS); Linares, George E. (CMS/OIS); Outerbridge, Monique (CMS/OIS); Oh, Mark U. (CMS/OIS); Chao, Henry (CMS/OIS); Warren, Kevin (CMS/OIS) ([Kevin.Warren@cms.hhs.gov](mailto:Kevin.Warren@cms.hhs.gov))

**Subject:** RE: Admin passwords and insecurity in healthcare.gov

Hello all,

Here is the feedback regarding this inquiry.

**Statement:**

CMS <sup>NotRes</sup><sub>p</sub> acknowledges the feedback by the security community. Analysis of the code and a review of the operational environment has confirmed that the site is secure and operating with low risk to consumers.

The code that has been reposted to Pastebin and commented on by TrustedSec is intended to be available to the public code as it makes the user interface (UI) of the site function. By design, these "resource bundles" contain all of the non-personalized text the user will see throughout the site. There is no admin level ID's or passwords located within the <sup>NotRes</sup><sub>p</sub> posted on-line. The code base at <sup>NotRes</sup><sub>Res</sub> has also just been queried for strings such as "admin password" and "abc123gov" per the twitter screenshot. No evidence was located that there is admin credential revealed. The person who retweeted with the abc password is just being humorous.

The <sup>NotRes</sup><sub>p</sub> and the SCA test team does run all of the tools mentioned in the article. A lot of commented code was removed prior to production, and the need to perform <sup>NotRes</sup><sub>Res</sub> is a roadmap item, in fact it is scheduled for release to the <sup>NotRes</sup><sub>Res</sub> environment tonight. Performing minification requires a lot of testing to ensure the application is not broken during <sup>NotRes</sup><sub>Res</sub> compression. . As <sup>NotRes</sup><sub>Res</sub> can be improved they will be release with subsequent builds.

To the other points in the article The marketplace does not use PHP so that is a non-issue. The use of Captcha was considered at one time, but removed to ensure 508-Compliance and to more importantly to remove burden on a consumer as *A Good Consumer Experience* was a design consideration. Also the concept of guessing ID's to see if there is a valid one or not is a known risk. We can look into taking steps at locking down access controls further, but it would negatively effect the user-experience.

Regards,

Tom Schankweiler, CISSP  
Information Security Officer, CCIO  
CMS\OIS\CIISG  
Consumer Information and Insurance Systems Group  
410-786-5956 (Balt. Office, N2-13-22)  
<sup>(b)(6)</sup> Mobile)

**From:** Charest, Kevin (OS/ASA/OCIO/OIS)

**Sent:** Thursday, October 10, 2013 12:21 PM



**To:** Fryer, Teresa M. (CMS/OIS); Schankweiler, Thomas W. (CMS/OIS)

**Cc:** Baitman, Frank (OS/ASA/OCIO)

**Subject:** FW: Admin passwords and insecurity in healthcare.gov

**Importance:** High

Teresa and Tom,

As you can see from the email chain below and the article at the Trustedsec site there are a significant number of concerns being raised here and they do appear to be legitimate even partially.

I need for you to review the current status of imbedded developer comment and ensure that they are removed. If – as is implied below, the admin password is something as absurd as what is in the tweet it be immediately changed and should be changed regularly in accordance with security standards and best practices.

Please let me know that you received this message and will be looking into for validation and remediation as soon as possible.

Kevin

Kevin Charest Ph.D., CISSP, PMP  
Chief Information Security Officer  
U.S. Department of Health and Human Services

Email: [Kevin.Charest@hhs.gov](mailto:Kevin.Charest@hhs.gov)

NotResp

Ofc. 202-690-5548; Mobile (b)(6)

*“Driving secure solutions through innovation and sustainable business practices”*

**From:** (b)(6)

**Sent:** Thursday, October 10, 2013 12:12 PM

**To:** Charest, Kevin (OS/ASA/OCIO/OIS)

**Cc:** (b)(6)

(b)(6)

**Subject:** Admin passwords and insecurity in healthcare.gov

**Importance:** High

Kevin,

NotResp



**TrustedSec** @TrustedSec

2h

Is the Affordable Health Care Website Secure? Probably not.  
trustedsec.com/october\_2013/a... #TrustedSec

Collapse

Reply Retweet Favorite \*\*\* More

**22**

RETWEETS

**3**

FAVORITES

(b)(6)

6:40 AM - 10 Oct 13 · Details

45m

(b)(6)

(b)(6)

comments in tha

NotResp

Details

(b)(6)

Message

**From:** Schankweiler, Thomas W. [NotResp]  
[NotResp]  
on behalf of Schankweiler, Thomas W. (CMS/OIS)  
**Sent:** 10/10/2013 9:55:16 PM  
**To:** James, Brian M. (CMS/CCIO) [NotResp]  
**CC:** Brackett, Stacie D. (CMS/CCIO) [NotResp]  
[NotResp] Lyles, Darrin V. (CMS/OIS) (Darrin.Lyles@cms.hhs.gov)  
[NotResp]  
'Duane.Cummings@cgifederal.com' [Duane.Cummings@cgifederal.com]  
**Subject:** FW: Admin passwords and insecurity in healthcare.gov  
**Importance:** High

Brian,

I need your contractors to look at this as it relates to the finder page and provide a response by noon Friday. This has attention of the HHS CIO, CMS CIO, and the HHS OIG. An initial response has been provided, but I need your feedback on the Finder page.

[https://www.trustedsec.com/october\\_2013/affordable-health-care-website-secure-probably/](https://www.trustedsec.com/october_2013/affordable-health-care-website-secure-probably/) and take a look at the comments to the post pictured below, on twitter (<https://twitter.com/TrustedSec/statuses/388298092971163648>).

Thanks,

Tom

**From:** Quaintance, Eric (CGI Federal) [mailto:Eric.Quaintance@cgifederal.com]  
**Sent:** Thursday, October 10, 2013 3:42 PM  
**To:** Schankweiler, Thomas W. (CMS/OIS)  
**Subject:** RE: Admin passwords and insecurity in healthcare.gov

Hi Tom, one add'l bit of information regarding "CKEditor" as referenced here:  
[https://www.trustedsec.com/october\\_2013/affordable-health-care-website-secure-probably/](https://www.trustedsec.com/october_2013/affordable-health-care-website-secure-probably/)

The URL depicted in the Google search results specifies **finder.healthcare.gov**. **Finder** is not part of our project.

**Eric Quaintance**

Healthcare & Compliance | Application Security | H&CP Security Practice  
x27.4654 / 610.842.5094 | Herndon: near rm3041 | Fairfax: 6th West-001A

**From:** Schankweiler, Thomas W. (CMS/OIS) [mailto:thomas.schankweiler@cms.hhs.gov]  
**Sent:** Thursday, October 10, 2013 2:14 PM  
**To:** Quaintance, Eric (CGI Federal)  
**Subject:** Fw: Admin passwords and insecurity in healthcare.gov

Fyi

**From:** Schankweiler, Thomas W. (CMS/OIS)

**Sent:** Thursday, October 10, 2013 02:08 PM

**To:** Fryer, Teresa M. (CMS/OIS)

**Cc:** Ashbaugh, Jason L. (CMS/OIS); Linares, George E. (CMS/OIS); Outerbridge, Monique (CMS/OIS); Oh, Mark U. (CMS/OIS); Chao, Henry (CMS/OIS); Warren, Kevin (CMS/OIS) (Kevin.Warren@cms.hhs.gov)

**Subject:** RE: Admin passwords and insecurity in healthcare.gov

Hello all,

Here is the feedback regarding this inquiry.

**Statement:**

**CMS [NotRes] acknowledges the feedback by the security community. Analysis of the code and a review of the operational environment has confirmed that the site is secure and operating with low risk to consumers.**

The code that has been reposted to Pastebin and commented on by TrustedSec is intended to be available to the public code as it makes the user interface (UI) of the site function. By design, these "resource bundles" contain all of the non-personalized text the user will see throughout the site. There is no admin level ID's or passwords located within the [NotRes] posted on-line. The code base at [NotRes] has also just been queried for strings such as "admin password" and "abc123gov" per the twitter screenshot. No evidence was located that there is admin credential revealed. The person who retweeted with the abc password is just being humorous.

The [NotRes] and the SCA test team does run all of the tools mentioned in the article. A lot of commented code was removed prior to production, and the need to perform [NotRes] is a roadmap item, in fact it is scheduled for release to the [NotRes] environment tonight. Performing minification requires a lot of testing to ensure the application is not broken during [NotRes] compression. . As [NotRes] can be improved they will be release with subsequent builds.

To the other points in the article The marketplace does not use PHP so that is a non-issue. The use of Captcha was considered at one time, but removed to ensure 508-Compliance and to more importantly to remove burden on a consumer as *A Good Consumer Experience* was a design consideration. Also the concept of guessing ID's to see if there is a valid one or not is a known risk. We can look into taking steps at locking down access controls further, but it would negatively effect the user-experience.

Regards,

Tom Schankweiler, CISSP

Information Security Officer, CCIO

CMS\OIS\CIISG

Consumer Information and Insurance Systems Group

410-786-5956 (Balt. Office, N2-13-22)

[b)(6)] (Mobile)

**From:** Charest, Kevin (OS/ASA/OCIO/OIS)  
**Sent:** Thursday, October 10, 2013 12:21 PM  
**To:** Fryer, Teresa M. (CMS/OIS); Schankweiler, Thomas W. (CMS/OIS)  
**Cc:** Baitman, Frank (OS/ASA/OCIO)  
**Subject:** FW: Admin passwords and insecurity in healthcare.gov  
**Importance:** High

Teresa and Tom,

As you can see from the email chain below and the article at the Trustedsec site there are a significant number of concerns being raised here and they do appear to be legitimate even partially.

I need for you to review the current status of imbedded developer comment and ensure that they are removed. If -- as is implied below, the admin password is something as absurd as what is in the tweet it be immediately changed and should be changed regularly in accordance with security standards and best practices.

Please let me know that you received this message and will be looking into for validation and remediation as soon as possible.

Kevin

Kevin Charest Ph.D., CISSP, PMP  
Chief Information Security Officer  
U.S. Department of Health and Human Services

Email: Kevin.Charest@hhs.gov

NotResp

Ofc. 202-690-5548; Mobile: (b)(6)

*"Driving secure solutions through innovation and sustainable business practices"*

**From:** (b)(6)  
**Sent:** Thursday, October 10, 2013 12:12 PM  
**To:** Charest, Kevin (OS/ASA/OCIO/OIS)  
**Cc:** (b)(6)  
(b)(6)  
**Subject:** Admin passwords and insecurity in healthcare.gov  
**Importance:** High

Kevin,

NotResp



**TrustedSec** @TrustedSec

2h

Is the Affordable Health Care Website Secure? Probably not.

trustedsec.com/october\_2013/a... #TrustedSec

Collapse

Reply Retweet Favorite More

**22**

RETWEETS

**3**

FAVORITES

(b)(6)

6:40 AM - 10 Oct 13 · Details

45m

(b)(6)

(b)(6)

comments in tha

NotResp

Details

(b)(6)

Message

**From:** Schankweiler, Thomas W. (CMS/OIS) [NotResp]  
[NotResp]  
on behalf of Schankweiler, Thomas W. (CMS/OIS)  
**Sent:** 11/25/2013 6:52:16 PM  
**To:** Coutts, Todd (CMS/OIS) [NotResp]  
[NotResp]  
**Subject:** RE: Security Items - Familiar?

Yes, we need these items worked as defects. We can work next to prioritize them, but I was told to get all our security items on the list so that they can be addressed. We are working now to get as many of them as possible cleaned up.

Tom

**From:** Coutts, Todd (CMS/OIS)  
**Sent:** Sunday, November 24, 2013 3:52 PM  
**To:** Schankweiler, Thomas W. (CMS/OIS)  
**Subject:** Security Items - Familiar?  
**Importance:** High

Tom,

A few questions for you:

1. Are you familiar with the Security items in the extract from Remedy below?
2. If so, do you know if these are already being worked?
3. If not, how would you like to handle them to make sure they get worked? Do you want to work together to get them initiated?

**Todd Coutts**

Centers for Medicare & Medicaid Services  
Office of Information Services  
301-492-5139 (office) [Redacted] (b)(6) (mobile) | [todd.coutts1@cms.hhs.gov](mailto:todd.coutts1@cms.hhs.gov)  
7700 Wisconsin Ave Bethesda MD 20814 | Location: 9308

**From:** Jones, Lynn B. [mailto:lbjones@mitre.org]  
**Sent:** Sunday, November 24, 2013 10:59 AM  
**To:** Coutts, Todd (CMS/OIS)  
**Cc:** Holden, Stacey (CMS/OIS); Cole, Reba R. (CMS/OIS)  
**Subject:** IMPORTANT - Decision on [Redacted] tickets for CCB.  
**Importance:** High

I looked at yesterday's Remedy tickets and there are E&E tickets and some Infrastructure/App Security tickets. The non-[Redacted] tickets are all very serious and security related.

Do you want ALL of these on the CCB list? I tend to believe we could just assign them and move on. However, they probably need to be made aware of them. Should these be added to the agenda. It looks to me like they are LIKELY included in the '65' or perhaps should be if they are not.

Here is the info for the [Redacted] tickets from this morning:

(b)(5)



(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)



(b)(5)

(b)(5)

(b)(5)

Lynn B. Jones  
Principal Multi-Disciplinary Systems Engineer  
The MITRE Corporation

Cell (b)(6)

Message

**From:** Schankweiler, Thomas W. (CMS/OIS); [Redacted] NotResp

on behalf of [Redacted] NotResp

**Sent:** 12/12/2013 10:23:30 PM

**To:** Booth, Jon G. (CMS/OC); [Redacted] NotResp

Linares, George E. (CMS/OIS); [Redacted] NotResp

**CC:** [Redacted] NotResp

Outerbridge, Monique (CMS/OIS); [Redacted] NotResp

[Redacted] NotResp; Grothe, Kirk A. (CMS/OIS); [Redacted] NotResp

[Redacted] NotResp; Nelson, David J. (CMS/OEM); [Redacted] NotResp

[Redacted] NotResp; ryer, Teresa M. (CMS/OIS)

[Redacted] NotResp

**Subject:** FW: [Redacted] NotResp

Mr. CTO, and Jon B.

I understand what Ryan is requesting and why he wants to request this information, but brining in another application to monitor web page performance is probably not necessary. I am also thinking that one of the existing web tools from OC should be able to do what Ryan is asking for. I am not sure who exactly to raise this to, but at this point I am not in favor (from a security perspective of course)of Ryan's technical approach.

Could you please advise.

Thanks,

Tom

**From:** Ramamoorthy, Balaji Manikandan (CGI Federal) [mailto:balajimanikandan.ramamoorthy@cgifederal.com]

**Sent:** Thursday, December 12, 2013 5:00 PM

**To:** Panchadsaram, Ryan (HHS/ONCIT)

**Cc:** [Redacted] NotResp; Schankweiler, Thomas W. (CMS/OIS); Quaintance, Eric (CGI Federal); Dhas, Navin (CGI Federal); Shenoy, Dilip (CGI Federal)

**Subject:** RE: [Redacted] NotResp

Hi Ryan,

Currently FFM sets the header [Redacted] NotResp to prevent against clickjacking attacks. This allows the marketplace to be framed only under healthcare.gov. The only way to add optimizely.com to the whitelist would be setting the value to [Redacted] NotResp

Introducing this option would increase risk in two ways.

Firstly, it would increase the reliance on Optimizely's security posture. By allowing *healthcare.gov* to be rendered in an iframe on optimizely.com, it opens the site up to [Redacted] NotResp. An attacker could use a weakness in Optimizely.com to potentially [Redacted] NotResp although this scenario is less likely than other attack scenarios the risk and reliance on Optimizely's security posture is increased.

The second area of risk that is increased is due to the lack of cross platform support for the **NotResp**

**NotResp** This option is not widely supported across all browsers. In some browsers the default behavior is to fail-open. In this case, the browser **NotResp**

**NotResp** This could lead to users of browsers that do not support the **NotResp**

**NotResp**

Here is the matrix of the browser support for the ALLOW-FROM header value for reference.

Browser	DENY/SAMEORIGIN Support Introduced	ALLOW-FROM Support Introduced
Chrome	<b>NotResp</b>	
Firefox (Gecko)		
Internet Explorer		
Opera		
Safari		

I have copied Tom on this email who can weigh in on the risks described here.

Thanks

Balaji M. Ramamoorthy

**From:** Panchadsaram, Ryan

**Sent:** Thursday, December 12, 2013 12:26 PM

**To:** Ramamoorthy, Balaji Manikandan (CGI Federal)

**Cc:** **NotResp**

**Subject:** **NotResp**

Thank you!

---  
**Ryan Panchadsaram** | [ryan.panchadsaram@hhs.gov](mailto:ryan.panchadsaram@hhs.gov) | 415-413-8270

**From:** <Ramamoorthy>, "Balaji Manikandan (CGI Federal)" <[balajimanikandan.ramamoorthy@cgifederal.com](mailto:balajimanikandan.ramamoorthy@cgifederal.com)>

**Date:** Thursday, December 12, 2013 at 11:58 AM

**To:** Ryan Panchadsaram <[ryan.panchadsaram@hhs.gov](mailto:ryan.panchadsaram@hhs.gov)>

**Cc:** "<[cgiadhocteam@googlegroups.com](mailto:cgiadhocteam@googlegroups.com)>" <[cgiadhocteam@googlegroups.com](mailto:cgiadhocteam@googlegroups.com)>

**Subject:** RE: **NotResp**

Hi Ryan,

I am looking into this request and determining the security risks that might be involved. I will get back to before COB with the details.

Thanks

Balaji M. Ramamoorthy

**From:** Panchadsaram, Ryan  
**Sent:** Thursday, December 12, 2013 11:57 AM  
**To:** Panchadsaram, Ryan; Ramamoorthy, Balaji Manikandan (CGI Federal)  
**Cc:** [cgiaidhocteam@googlegroups.com](mailto:cgiaidhocteam@googlegroups.com)  
**Subject:** Re: [Redacted] NotResp

Hi Balaji – I got your out of office message yesterday. Is this something we can discuss and resolve today?

---  
Ryan Panchadsaram | [ryan.panchadsaram@hhs.gov](mailto:ryan.panchadsaram@hhs.gov) | 415-413-8270

**From:** <Panchadsaram>, Ryan Panchadsaram <[ryan.panchadsaram@hhs.gov](mailto:ryan.panchadsaram@hhs.gov)>  
**Date:** Wednesday, December 11, 2013 at 10:40 PM  
**To:** "balajimanikandan.ramamoorthy@cgifederal.com" <[balajimanikandan.ramamoorthy@cgifederal.com](mailto:balajimanikandan.ramamoorthy@cgifederal.com)>  
**Cc:** "cgiaidhocteam@googlegroups.com" <[cgiaidhocteam@googlegroups.com](mailto:cgiaidhocteam@googlegroups.com)>  
**Subject:** FW: [Redacted] NotResp

Hi Balaji -

We are trying to use a tool for running experiments on how we can improve the throughput of HealthCare.gov. One of the tools we would like to use is Optimizely. To use their editing tool we need to enable the access of HealthCare.gov in an iFrame.

[Redacted] NotResp

More instructions are below from Optimizely support. If you need more information from me, just ask. Or if you need me to work with someone else.

Best,  
Ryan

---  
Ryan Panchadsaram | [ryan.panchadsaram@hhs.gov](mailto:ryan.panchadsaram@hhs.gov) | 415-413-8270

**From:** <Booth>, "Jon G. (CMS/OC)" <[Jon.Booth@cms.hhs.gov](mailto:Jon.Booth@cms.hhs.gov)>  
**Date:** Wednesday, December 11, 2013 at 4:37 PM  
**To:** Ryan Panchadsaram <[ryan.panchadsaram@hhs.gov](mailto:ryan.panchadsaram@hhs.gov)>  
**Subject:** Re: [Redacted] NotResp

Yes, I'd recommend starting with Balaji. Let me know if you need his contact info.

**From:** <Panchadsaram>, "Ryan (HHS/ONCIT)" <[Ryan.Panchadsaram@hhs.gov](mailto:Ryan.Panchadsaram@hhs.gov)>  
**Date:** Wednesday, December 11, 2013 at 4:34 PM  
**To:** Jon Booth <[jon.booth@cms.hhs.gov](mailto:jon.booth@cms.hhs.gov)>  
**Subject:** Re: [Redacted] NotResp

Ahh. So Akamai controls that.

Is there someone at CGI that I should make the request to for the exception to Optimizely?

---  
Ryan Panchadsaram | [ryan.panchadsaram@hhs.gov](mailto:ryan.panchadsaram@hhs.gov) | 415-413-8270

**From:** <Booth>, "Jon G. (CMS/OC)" <[Jon.Booth@cms.hhs.gov](mailto:Jon.Booth@cms.hhs.gov)>

**Date:** Wednesday, December 11, 2013 at 4:22 PM

**To:** Ryan Panchadsaram <[ryan.panchadsaram@hhs.gov](mailto:ryan.panchadsaram@hhs.gov)>

**Subject:** Re: [Redacted] NotResp

This block was implemented per direction from the CGI security team. I will forward you the thread.

**From:** <Panchadsaram>, "Ryan (HHS/ONCIT)" <[Ryan.Panchadsaram@hhs.gov](mailto:Ryan.Panchadsaram@hhs.gov)>

**Date:** Wednesday, December 11, 2013 at 4:15 PM

**To:** Jon Booth <[jon.booth@cms.hhs.gov](mailto:jon.booth@cms.hhs.gov)>

**Subject:** FW: [Redacted] NotResp

Hi Jon – I was working with Optimizely tech support to figure out why our stuff wasn't working. It seems we block hc.gov from being shown in iFrames? Are you aware that we do that block? If so – then it seems we have to add it to a whitelist...

---  
Ryan Panchadsaram | [ryan.panchadsaram@hhs.gov](mailto:ryan.panchadsaram@hhs.gov) | 415-413-8270

**From:** Optimizely Support <[support@optimizely.com](mailto:support@optimizely.com)>

**Reply-To:** Optimizely Support <[support@optimizely.com](mailto:support@optimizely.com)>

**Date:** Wednesday, December 11, 2013 at 4:07 PM

**To:** Ryan Panchadsaram <[ryan.panchadsaram@hhs.gov](mailto:ryan.panchadsaram@hhs.gov)>

**Subject:** Re: [Redacted] NotResp

## - Please type your reply above this line -##

**Gary (Optimizely Support)**

Dec 11 01:07 PM (PST)

Hi Ryan,

When loading that login page I found an error as follows, which is the root of your problem. The best way to solve this is to have your developer [Redacted] NotResp o allow us to load your page inside an iframe:

Refused to display

'https:' [Redacted] NotResp

[Redacted] NotResp

More details:

This MSDN Blog article clearly explains what the [Redacted] NotResp does and how it can be



NotResp

The notable excerpt is here:

Web developers can send a

NotResp

responses to restrict how the page may be framed.

#### Token Values

The X-Frame-Options header may contain one of three tokens:

- DENY
- SAMEORIGIN
- ALLOW-FROM origin

If the value contains the token SAMEORIGIN, the browser will block rendering only if the origin of the top-level browsing-context is different than the origin of the content containing the X-FRAME-OPTIONS directive. For instance, if <http://shop.example.com/confirm.asp> contains the X-FRAME-OPTIONS directive with the SAMEORIGIN token, the page may be framed by any page from the exact<http://shop.example.com> origin.

If the value contains the token ALLOW-FROM origin, the browser will block rendering only if the origin of the top-level browsing context is different than the origin value supplied with the Allow-From directive. For instance, if <http://shop.example.com/confirm.asp> contains the X-FRAME-OPTIONS directive with the value Allow-From <https://partner.affiliate.com>, then the page may be framed only by pages from the <https://partner.affiliate.com> origin.

NotResp

Let me know how I can help,  
Gary

On a scale of 1 to 10, how happy are you with my response? Click below to rate:

(Worst)12345678910(Best)

Interested in learning more? Sign up for the next installment of our free Customer Onboarding Webinar Series!

-----  
Here's a recap of what we've already discussed:

Panchadsaram, Ryan (HHS/ONCIT) commented on Dec 10:

Hi Gary -

I tried that – and it still gives that same message. :(

You can repro – you don't have to login – try looking at this page: <https://>

NotResp

This is what it looks like it Optimizely:

Gary commented on Dec 10:

Hi Ryan,

Did the firewall workaround work for you? Please navigate to the page in an adjacent Tab, browse through to the page by logging in (or completing the necessary steps to be cookie'd & cleared), then copy the URL, open a new tab & start a new experiment with the target URL. Every time you want to make changes & see the page in the Editor you will have to browse to the page in an adjacent tab before opening the Experiment.

If this doesn't work, I'd like to take a look at your page, so please send me a login I can use for testing.

Let me know how I can help,

Gary

Panchadsaram, Ryan (HHS/ONCIT) commented on Dec 10:

We added the snippet:

But I'm still seeing:

Any other things I should try?

-----

Ryan Panchadsaram | [ryan.panchadsaram@hhs.gov](mailto:ryan.panchadsaram@hhs.gov) | 415-413-8270

Gary commented on Dec 10:

Hi Ryan,

Pretty cool to see you guys are using our product!

So I'm seeing the page is behind a firewall and I have to log in. Without logging in, I can't test out the page, so my question is are you unable to load the page in the Optimizely Editor? If so, here's the workaround. If not, can you send me a log in and screenshot of what you're trying to modify?

You'll have to [Install the Snippet](<http://>  
load the page in the Optimizely Editor.

NotResp

to the target page(s) and then

To load a shopping cart page with an element in it, or or load a logged in page, Optimizely treats this like a firewall. To bypass this firewall, please navigate to the page in an adjacent Tab, browse through to the page by logging in (or completing the necessary steps to be cookie'd & cleared), then copy the URL, open a new tab & start a new experiment with the target URL. Every time you want to make changes & see the page in the Editor you will have to browse to the page in an adjacent tab before opening the Experiment.

What this does is provide your browser session with the information necessary to give you proper access to that page; sometimes this access is information stored in a cookie, which you must perform the correct actions to be passed that cookie with the proper values.

Let me know how I can help,  
Gary

Panchadsaram, Ryan (HHS/ONCIT) commented on Dec 10:

Hi Optimizely!

We are trying to use your product for a few sections of HealthCare.gov. We are hoping it can help increase throughput and run a few experiments.

When I try to do an experiment on: <http://>

NotResp

It doesn't render the main app area. I can't figure out why...any pointers would be appreciated.

Best,

Ryan

---

Ryan Panchadsaram | [ryan.panchadsaram@hhs.gov](mailto:ryan.panchadsaram@hhs.gov) | 415-413-8270

Interested in finding out more? Head on over to our [Knowledge Base](#)

--

You received this message because you are subscribed to the Google Groups "cgiahdhocteam" group.

To unsubscribe from this group and stop receiving emails from it, send an email to [cgiahdhocteam+unsubscribe@googlegroups.com](mailto:cgiahdhocteam+unsubscribe@googlegroups.com).

For more options, visit [https://groups.google.com/groups/opt\\_out](https://groups.google.com/groups/opt_out).

## Message

**From:** Schankweiler, Thomas W. (CMS/OIS) [NotResp]  
 [NotResp]  
 on behalf of Schankweiler, Thomas W. (CMS/OIS)  
**Sent:** 1/31/2014 8:30:13 PM  
**To:** Youd, Hank (CMS/CTR) [NotResp]  
 [NotResp] Basavaraju, Venkat (CMS/OIS) [NotResp]  
 [NotResp] Purcell, Timothy J. (CMS/OIS)  
 [NotResp]  
**CC:** Warren, Kevin (CMS/OIS) [NotResp]  
 [NotResp]  
**Subject:** RE: EIDM Ticket information  
**Attachments:** Karlton Kim

Hank and Kevin,

App.prod may be OC

The hub one may be ffm, you all would need to look at the additional details in the remedy ticket. Contact Karlton Kim.  
 I would need more details on to recommend who to assign them to.

Tom

**From:** Youd, Hank (CMS/CTR)  
**Sent:** Friday, January 31, 2014 1:31 PM  
**To:** Basavaraju, Venkat (CMS/OIS); Purcell, Timothy J. (CMS/OIS)  
**Cc:** Schankweiler, Thomas W. (CMS/OIS); Warren, Kevin (CMS/OIS)  
**Subject:** EIDM Ticket information

The following has been identified to be owned by your group. We are looking to get information for each item listed below that include:

- When can these be fixed (date)?
- What is the CR#?
- Provide a description of the fix?

INC00000263 2912	Critical	RIDP allows you to put in anyone's information to PHISH for experian questions	EIDM, they should resolve or agree to put this in their Risk Assessment report
none	Critical	RIDP allows you to use someone else's information and it will overwrite the data you used when initially creating your account	How does this not have a remedy ticket? Someone needs to show this to EIDM
INC00000269 2817	High	EIDM Vulnerabilities artf137815 : CAT 8, EIDM, eidm.cms.gov, GET and POST XSS	EIDM

INC000002632926	High	Cross Site Scripting / <a href="https://eidmi.cms.gov/EIDMlogin/loginpage.action">https://eidmi.cms.gov/EIDMlogin/loginpage.action</a> (vuln POST parameter "request_id")	EIDM
INC000002693041	Medium	<a href="https://eidmi.cms.gov/identity/faces/accountlocked">https://eidmi.cms.gov/identity/faces/accountlocked</a> allows a user to enter any username and view security questions.	EIDM

Would you know who the correct contact is for the following?

INC000002693051	Medium	<a href="https://app.prod.healthcare.gov/access/oblix/apps/webgate/bin/webgate.cgi?progid=1">https://app.prod.healthcare.gov/access/oblix/apps/webgate/bin/webgate.cgi?progid=1</a> Exposes server names	?
INC000002693058	Medium	artf157249 : CAT 7, Log File Configuration Issues	?
INC000002693059	Medium	artf147578 : CAT 7, HUB, hub.cms.gov, Vulnerable to XSS	?
INC000002692824	High	Files were discovered that contained passwords, certificates etc	?

Thank you,

Hank Youd (Contractor)

(703)354-2229 x550 (Direct)

(b)(6) (Mobile)

NotRe  
CMS SP Security Team

Consumer Information & Insurance Systems Group (CIISG)

Centers for Medicare & Medicaid Services (CMS)

To report a security incident, please contact the:

CMS Marketplace Security Team

Consumer Information & Insurance Systems Group (CIISG)

Centers for Medicare & Medicaid Services (CMS)

Phone - 703-594-4961 NotResp (24/7 coverage)

NotResp

#### DISCLAIMER:

THE INFORMATION CONTAINED IN THIS MESSAGE AND ANY FILE TRANSMITTED WITH IT IS INTENDED ONLY FOR THE USE OF THE INDIVIDUAL OR ENTITY TO WHICH IT IS ADDRESSED AND MAY CONTAIN INFORMATION THAT IS PRIVILEGED, CONFIDENTIAL, AND EXEMPT FROM DISCLOSURE. Any disclosure, distribution, copying or use of the information by anyone other than the intended recipient, regardless of address or routing, is strictly prohibited. If you have received this message in error, please advise the sender by immediate reply and delete the original message. Personal messages express views solely of the sender and are not attributable to the company.

## Meeting Agenda – Pre-Deployment ORR/PRR

Wednesday, September 25, 2013, 8:30 AM – 12:30 PM

### Overview

Logistics	Goals for Review
<p>1. <b>Baltimore Location:</b> MITRE Baltimore 2275 Rolling Road Outside CMS North Gate-BS104</p> <p>2. <b>Bethesda 7700 Wisconsin Location:</b> 7700 Bldg. Tokyo (9407 (VTC to MITRE room)</p> <p>3. <b>Bethesda 7501 Location:</b> Pentagon City (0980) 9th Floor (VTC to MITRE room)</p> <p>4. <b>Webinar:</b> (b)(6)</p> <p>5. <b>Phone:</b> (b)(6)</p>	<ul style="list-style-type: none"> <li>Ensure that we are ready for: <ul style="list-style-type: none"> <li>Marketplace IT operations</li> <li>The production deployment activities</li> </ul> </li> <li>Make sure that all stakeholders understand the IT functionality available for 10/1 and the operational implications.</li> </ul>

### Overall Organization of the September 20<sup>th</sup> and September 25<sup>th</sup> Sessions

Topic	Time dedicated on 9/20	Time dedicated on 9/25
End-to-End Scenarios Checklist	20 minutes	20 minutes
Functionality & Interface Checklist	4 hours	1 hour
Non Functional Development Checklist	None	30 minutes
Security Checklist	None	30 minutes
Data Preparation Checklist	30 minutes	30 minutes
Welcome/Breaks/Lunch	45 minutes	30 minutes
Section 508 Compliance	0 minutes	30 minutes
Performance & Stress Testing Checklist	None	30 minutes
Elasticity & Scalability Checklist	None	30 minutes
Environments and Infrastructure Checklist	1 hour	None (Note: handling in separate, smaller meeting)
Agreements Checklist	None	1 hour
Issuer, Federal, State, Agent/Broker Checklist	None	1 hour
Operations	2 hours	None (Note: handling in separate, smaller meeting)
<b>TOTAL</b>	<b>8.5 hours</b>	<b>4 hours</b>

Agenda Item	Reporting Out	Time	Guidance
Check in	N/A	8:30 – 8:45	<ul style="list-style-type: none"> <li>Sign the attendance sheet</li> </ul>
Welcome	<ul style="list-style-type: none"> <li>Component senior leadership</li> <li>Todd Coutts (agenda and ground rules)</li> </ul>	8:45 – 9:00	<ul style="list-style-type: none"> <li><b>Note:</b> aggressive timeslots to compress the meeting into half a day.</li> </ul>
End-to-End Scenario Checklist	<ul style="list-style-type: none"> <li>Business: Sarah Boehm (CCIO), Ben Walker (CCIO), Bill Trefzger (OC)</li> <li>IT: Mark Oh (OIS), Ketan Patel (OC)</li> </ul>	9:00 – 9:20	<p>GENERAL GUIDANCE</p> <ul style="list-style-type: none"> <li>Has there been a successful walkthrough of the three end-to-end scenarios?</li> <li>What did not work completely as planned that operations should know about?</li> </ul> <p>FOLLOW UP FROM LAST WEEK</p> <ul style="list-style-type: none"> <li>Financial Assistance scenarios <ul style="list-style-type: none"> <li>Correct eligibility determination (QHP vs. Medicaid/CHIP)?</li> <li>Eligibility results page?</li> <li>Eligibility notice?</li> </ul> </li> <li>Able to test without Test Harness / test data complications?</li> </ul>

Agenda Item	Reporting Out	Time	Guidance
Functionality & Interface Checklist			<ul style="list-style-type: none"> <li>OVERALL FOCUS <ul style="list-style-type: none"> <li>Provide updates from last week</li> </ul> </li> <li>QUESTIONS TO ANSWER: <ul style="list-style-type: none"> <li>What development was not completed?</li> <li>What is the operational impact of outstanding defects or incomplete requirements? <ul style="list-style-type: none"> <li>Help desk impact</li> <li>Business operations impact (e.g., Eligibility Support)</li> <li>Communications planning</li> <li>Business risk acceptance</li> </ul> </li> </ul> </li> <li>DO NOT: <ul style="list-style-type: none"> <li>Describe or debate the functionality or design of each function.</li> <li>Dwell on functions that were completely</li> </ul> </li> </ul>
My Account	<ul style="list-style-type: none"> <li>CMS Business: Susan Tudor (OC), Andrew Rumin (CCIIO)</li> <li>CMS IT: Ketan Patel (OC) /Venkat Basavaraju (OIS)</li> <li>Developer: CGI and QSSI EIDM</li> <li>Testing: ACA Independent Tester</li> </ul>	9:20 – 9:30	<ul style="list-style-type: none"> <li>Is it more stable than last week?</li> <li>Correct business rules implemented for issue found during Lite Account production (expiration of verification links)?</li> </ul>
Application	<ul style="list-style-type: none"> <li>CMS Business: Sarah Boehm (CCIIO)</li> <li>CMS IT: Steve Walter (OIS), Lijun Shao (OIS)</li> <li>Developer: CGI</li> <li>Testing: ACA Independent Tester</li> </ul>	9:30 –9:40	<ul style="list-style-type: none"> <li>More complex household scenarios working (more than 4 children on a plan)?</li> </ul>



Agenda Item	Reporting Out	Time	Guidance
Eligibility Determination	<ul style="list-style-type: none"> <li>• CMS Business: Ben Walker (CCIIO)</li> <li>• CMS IT: Steve Walter (OIS), Lijun Shao (OIS)</li> <li>• Developer: CGI and QSSI Hub</li> <li>• Testing: ACA Independent Tester and eGT Testing Team</li> </ul>	9:40 – 9:50	<ul style="list-style-type: none"> <li>• Core eligibility determination (QHP vs. Medicaid/CHIP assignments to wrong program)?</li> <li>• Verify Lawful Presence service?</li> <li>• Inconsistency and PEND logic?</li> </ul>
Plan Compare & Plan Select	<ul style="list-style-type: none"> <li>• CMS Business: Jack Lavelle (CCIIO), Patrick Flaherty (CCIIO), Lisa Ann Bailey (CCIIO)</li> <li>• CMS IT: Hung Van (OIS) / Bob Thurston (OIS Contractor)</li> <li>• Developer: CGI</li> <li>• Testing: ACA Independent Tester</li> </ul>	9:50 – 10:00	<ul style="list-style-type: none"> <li>• Compose Enrollment Groups (default &amp; custom groups)?</li> <li>• APTC allocation to the groups?</li> <li>• Plan Compare rating services for more than four children?</li> </ul>
Enrollment & Direct Enrollment	<ul style="list-style-type: none"> <li>• CMS Business: Jack Lavelle (CCIIO), Andrew Rumin (CCIIO)</li> <li>• CMS IT: Dan Miller (OIS), Hung Van (OIS) / Mike Cabral (OIS) / Bob Thurston (OIS Contractor)</li> <li>• Developer: CGI and QSSI Hub</li> <li>• Testing: ACA Independent Tester</li> </ul>	10:00 – 10:10	<ul style="list-style-type: none"> <li>• Two critical Direct Enrollment – secure redirect defects corrected?</li> <li>• Able to test without synthetic data with an 834/999 roundtrip?</li> </ul>
Call Center	<ul style="list-style-type: none"> <li>• CMS Business: Frances Harmatuk (OC)</li> <li>• CMS IT: Ketan Patel (OC) /Venkat Basavaraju (OIS)</li> <li>• Developer: CGI</li> <li>• Testing: ACA Independent Tester</li> </ul>	10:10 – 10:20	<ul style="list-style-type: none"> <li>• Call Center landing page: outstanding issue if a consumer starts with the Call Center?</li> <li>• Workaround for task escalation to Serco working OK?</li> </ul>

Agenda Item	Reporting Out	Time	Guidance
Eligibility Support – Case Management	<ul style="list-style-type: none"> <li>• CMS Business: Jacqueline Roche (CCIIO), Dave Nelson (OEM)</li> <li>• CMS IT: Becky Fender (OIS)</li> <li>• Developer: CGI, Serco</li> </ul>	10:20 – 10:30	<ul style="list-style-type: none"> <li>• Status of testing person view and person search?</li> <li>• Landing page?</li> <li>• Audit report?</li> </ul>
Other Update	<p>Reporting &amp; Metrics</p> <ul style="list-style-type: none"> <li>• CMS Business: Anne Pesto (CCIIO), Lori Maatta (OEM)</li> <li>• CMS IT: Glenn Radcliffe (OIS)</li> <li>• Developer: CACI</li> </ul> <p>Services for State Based Marketplaces (SBMs)</p> <ul style="list-style-type: none"> <li>• CMS IT: Mark Oh (OIS)</li> <li>• Developer: QSSI Hub</li> </ul> <p>HC.gov Learn Site</p> <ul style="list-style-type: none"> <li>• CMS Business: Jon Booth (OC)</li> </ul>	10:30 – 10:35	<ul style="list-style-type: none"> <li>• Any updates from last week?</li> </ul>
Non Functional Development Checklist	<ul style="list-style-type: none"> <li>• CMS IT: Bob Thurston (OIS Contractor)</li> </ul>	10:35 – 10:55	<ul style="list-style-type: none"> <li>• What should operations, Call Center and help desks be ready for in terms of user messages, error handling, etc?</li> </ul>
Performance & Stress Testing Checklist	<ul style="list-style-type: none"> <li>• CMS: Akhtar Zaman</li> <li>• Developers: CGI, QSSI Hub, QSSI EIDM</li> </ul>	10:55 – 11:15	<ul style="list-style-type: none"> <li>• What were the Performance &amp; Stress Testing Results?</li> <li>• What volume/capacity can the systems support?</li> </ul>

Agenda Item	Reporting Out	Time	Guidance
<b>Security Checklist</b>	<ul style="list-style-type: none"> <li>CMS: Tom Schankweiler (OIS)</li> </ul>	11:15 – 11:30	<ul style="list-style-type: none"> <li>Where do we stand in terms of Security Controls Assessment (SCA) and Authority to Operate (ATO)?</li> </ul>
<b>Agreements Checklist</b>	<ul style="list-style-type: none"> <li>Tom Schankweiler (OIS), Daniel Lazenby (OIS), Reba Cole (OIS), Nancy Keates (OIS)</li> </ul>	11:30 – 11:50	<ul style="list-style-type: none"> <li>Where do we stand with agreements and Authority to Connect?</li> <li>Risks?</li> </ul>
<b>Issuer, Federal, State, Agent/Broker Checklist</b>	<p>Issuer:</p> <ul style="list-style-type: none"> <li>Beth Paris, CCIO (Issuer Agreements)</li> <li>Walt Dill (Onboarding)</li> </ul> <p>Agent/Broker:</p> <ul style="list-style-type: none"> <li>Pete Nakahata (CCIO)</li> <li>Bing Chao (OIS)</li> </ul> <p>State Onboarding</p> <ul style="list-style-type: none"> <li>Walt Dill (OIS)</li> </ul> <p>Federal</p> <ul style="list-style-type: none"> <li>Richard Speights (OIS)</li> </ul>	11:50 – 12:10	<ul style="list-style-type: none"> <li>Where do we stand with onboarding Issuers, States, Agent/Brokers, and Federal Agencies?</li> </ul>
<b>Data Preparation Checklist</b>	<ul style="list-style-type: none"> <li>CMS: Mark Oh (OIS) and Doug Margush (OIS)</li> </ul>	12:10 – 12:20	<ul style="list-style-type: none"> <li>Walk through the checklist items and identify if items completed or what the plan is for completion.</li> </ul>
<b>Section 508</b>	<ul style="list-style-type: none"> <li>CMS: Jon Booth (OC)</li> </ul>	12:20 – 12:30	<ul style="list-style-type: none"> <li>Level of 508 compliance?</li> <li>Known 508 gaps.</li> </ul>

## WEEKLY PROJECT STATUS REPORT

CLIENT/PROJECT:	CMS/Enterprise Identity Management			YELLOW
PROJECT MANAGER:	Girish Shetty			
PROGRAM DIRECTOR:	Nitin Matta			
CLIENT CONTACT:	Deborah Seate, Venkat Basavaraju, Robert Burger, Todd Northwood, Sharlene Mansaray, Cathy Carter, Marc Richardson, Carla Jones, Tim Purcell, Mark Small			
STATUS PERIOD:	07/14/2013 to 07/21/2013			
STATUS SUMMARY				
TASKS COMPLETED /DELIVERIES FOR THIS PERIOD – 07/14/2013 to 07/21/2013				
Following are activities completed for this week:				
1. CR (Artifact artf147318): EIDM - PROD DB2 to DB1 swap was successfully implemented in the Production environment.				
2. Release 3 build 9 was successfully deployed in the Test environment.				
3. Completed the setup of EIDM Dev Environment with all EIDM specific customization				
4. QSSI EIDM team succesfully set up the Impl1 Environment and ran the test scripts successfully for EIDM specific dummy pages				
5. Database patching in the development environment NotResp				
6. QSSI EIDM team continue to build the BDC environment for the NotResp active active solution				
7. No Severity #1 or Severity #2 tickets currently opened in production. EIDM Helpdesk tickets status for this week:				
a. # of New Tickets Opened between 07/14/2013 to 07/21/2013 → 11				
b. # of Tickets Closed between 07/14/2013 to 07/21/2013 → 12 (Note: this number may include tickets opened from previous weeks).				
c. # of Tickets unresolved from 03/25/2013 to 07/21/2013 → 1				
8. QSSI supported ongoing application integration meetings for SHOP, CSR, FEM and Zone and shared meeting minutes as applicable. QSSI also supported Application integration meetings for the new applications in the pipeline like NotResp and shared meeting minutes.				
9. Testing of Release 3 Build 7 code in the Test environment.				
TASKS PLANNED/DELIVERIES FOR THIS PERIOD - 07/22/2013 to 07/28/2013				

1. Deploy EIDM Release 3 Build 9 in the Implementation and Production environment
2. zOne application to be integrated in the Production environment
3. Execute the performance testing effort in the Impl1 environment
4. Develop and Implement the new sub codes for Augmented Analytics provided by SAIC.
5. Continue building the BDC NOTR  
esp environment for the active active solution
6. Continue requirement gathering for new applications like NotResp integrating with EIDM
7. Continue Release 3 Build 9 testing and code fixes in the Test and Implementation Environment.
8. Analyze and Resolve outstanding issues in production, report delivery production status report on EIDM production and helpdesk operations.

**Scheduled Deployments in the EIDM Environment:**

Environment	Start Time	End Time	Activity
PROD	7/27/2013	7/27/2013	EIDM: Release 3 , zOne WaaS Application Integration Requested by CMS for 07/27 deployment instead of 07/28 deployment
IMPL	7/22/2013	7/22/2013	Release 3 Build #9, Zone updates Experian Phone numbers Provisioning users to application groups to get access to "My Profile" and "My Actions" from the Portal Home
IMPL 1	7/24/2013	8/6/2013	EIDM Performance testing

**EIDM Application Integration Status**

Applications	Current Status	Tentative Prod Date	CMS GTL
FFM	Testing in progress. EIDM team is working with CGI to resolve the issues found during testing.	July 28 <sup>th</sup> 2013	Susan Tudor/ Megan Reilly
Assister Integration (Agent Broker)	MLN data store details and connectivity details are still not finalized. EIDM team is still not certain of the requirements for Navigators and State workers.	August 15 <sup>th</sup> 2013	Mark Oh?
SHOP	Testing in progress. SHOP team is working on the firewall issues.	Sept 1 <sup>st</sup> 2013	Hannah Yoo



CSR	Testing in progress. Issues with <b>NotResp</b> and header attributes to be passed are being worked on. New <b>NotResp</b> attribute has been requested by CGI.	Sept 1 <sup>st</sup> 2013	Frances Harmatuk/ Jeffrey Burdette
MACPro	CR to be submitted for setting up the application/roles in EIDM Test Environment.	Dec 8 <sup>th</sup> 2013	Nancy Martin
Zone	<p>EIDM team provided sample zONE users (BOR, Helpdesk, Approver and end user) which enabled zONE team to test the authentication and log into zONE using EIDM. EIDM successfully bulk uploaded the zONE sample users in the EIDM TEST environment. EIDM is waiting on confirmation from the zONE team to receive the user type list.</p> <p>The following technical issues were resolved:</p> <ul style="list-style-type: none"> <li>➤ The firewall issue causing the zONE test URL to toggle between two sites has been fixed.</li> <li>➤ zONE application successfully received the EIDM user id via <b>NotResp</b> plug-in and was also able to receive the header variables for authenticated user via EIDM.</li> <li>➤ EIDM team provided SSO logout info to the zONE team.</li> </ul>	July 28 <sup>th</sup> 2013	Damon Underwood
ASP	<p>Updates for this week:</p> <ul style="list-style-type: none"> <li>➤ EIDM provided updated process flows; business owner approval is pending.</li> <li>➤ The process for setting up 'My Actions' functionality was reviewed with the ASP team.</li> <li>➤ A CR for setting up <b>NotResp</b> in the EIDM Test environment will be sent next week.</li> </ul>	Dec 15 <sup>th</sup> 2013	Sarah Harding
QMAT	<p>Testing in progress in EIDM test environment. Some issues like requesting QMAT approver roles were generating errors due to some coding and development team is working to resolve the same.</p> <p>Business decision to have MFA included is still awaiting confirmation.</p>	Dec 15 <sup>th</sup> 2013	Falk Paige
ASETT	<p>Updates for this week:</p> <ul style="list-style-type: none"> <li>➤ ASETT proposed having 2 End User roles – Registrant 1 and Registrant 2.</li> <li>➤ EIDM recommended that the Registrant enter the ASETT 2 User ID during the role request process, since that info is required to access the user's case.</li> <li>➤ EIDM will explore how to technically send the ASETT 2 User ID to ASETT (i.e. – header variable).</li> <li>➤ ASETT provided the layout of the Special Code lookup table for the role request process. Further discussion is needed on connectivity.</li> </ul>	March 2 <sup>nd</sup> 2014	Gladys Wheeler
Open Payments	No update this week.	March 2014	
EPPE	No update this week; Meeting needs to be scheduled.	March 2 <sup>nd</sup> 2014	
QIES	Follow-up meeting needs to be scheduled to discuss technical questions and other details.	2015	Jack Williams?

PROPOSED SCOPE FOR RELEASE 3						
<b>Release 3:</b> <ul style="list-style-type: none"> <li>EIDM Web Services to support Consumer Portal, CSR and SHOP Integration with EIDM.</li> <li>Implementation of Federation to integrate CSR users.</li> <li>Implement WaaS for integration of Agents, Brokers and Agents.</li> <li>Modify EIDM Step up process from LOA #1 to LOA #2 and LOA #3.</li> <li>Implement WaaS Database Connector.</li> </ul>						
HIGH LEVEL SCHEDULE FOR RELEASE 3 – WORK IN PROGRESS						
Will be listed in next weeks Status Report.						
ISSUES	DATE OPENED	PRIORITY	STATUS	CORRECTIVE ACTION		
1. EIDM Performance Testing issue. At present the Access Management and Identity lifecycle Management functions are not scaling beyond 250 CC users. EIDM Registration Services have been fine-tuned and is currently able to sustain 750 CC users with less than 1% error. On an average, EIDM can create around 9,000 users in an hour.	02/05/2013	High <b>Tracking Purposes: Affect the schedule for performance testing.</b>	Open	<p>Update on 07/21/2013: QSSI EIDM is on schedule with the Performance Testing effort. The new IMPL1 environment is complete. Scripts are complete as well and we will be running the scripts to get some baseline data on Sunday 07/21. There may be a scheduling conflict for the Performance center with the EDCG team. We have notified the EDCG team and are awaiting a response.</p> <p>Update on 07/14/2013: QSSI EIDM team is working on installing the OAM components in the EIDM Impl1 environment. QSSI EIDM team is also working with the EDCG team to get the scripts ready for the Performance testing effort. We are on schedule to complete the Testing effort by 07/31/2013.</p> <p>Update on 07/07/2013: Performance Test Plan will be shared with CMS by 07/09/2013.</p>		

				<p>QSSI EIDM team continues to work on the Impl1 environment.</p> <p>Update on 06/30/2013: With multiple deliveries of inaccurate operating systems for the VMs by URS, QSSI estimates the completion of the Implementation1 environment to be delayed by 2 weeks. QSSI is currently working on the Performance Test Plan with work load model and will submit the plan early next week for all the stakeholders to review. QSSI continues to work on the development of the the Impl1 environment.</p> <p>Update on 06/23/2013: Implementation environments were delivered by URS with an operating system version for the Database VM that did not match the existing requirement for EIDM DB environments. Expected delivery is now 06/25/2013, which has delayed the performance testing timelines. QSSI has requested for a meeting with all stake holders to ensure participation from all stake holders and confirm that everyone is in consensus with the activities scheduled for the Performance Testing effort. As an continued effort, QSSI is working with EDCG team in building the Impl1 environment.</p> <p>Update on 06/16/2013: QSSI has provided a high level schedule for all the tasks in Performance Testing and requested a meeting for early next with all the parties involved in the effort. The meeting is to ensure everyone understands what is involved in the testing effort, clearly discuss the expectations from all stakeholders, and what metrics would be collected for the same.</p> <p>Update on 06/10/2012: No further updates. We are still waiting on Doug to provide the compute.</p>
--	--	--	--	--



					<p>Update on 5/24/2012: CMS decided on setting up a second instance of IMP environment to conduct the performance testing specifically to scale the <b>NOTRe</b> component. QSSI is working with Doug Margush to provide the server details.</p> <p>Update on 05/17/2013: Awaiting CMS response on QSSI request for a dedicated implementation environment to execute performance testing. At this time performance testing scheduled for 5/20/2013 is put on hold. Received confirmation from CMS ETC team that performance testing can be executed up to 10,000 concurrent users at CMS ETC.</p> <p>Updated on 04/29/2013: Scheduling of performance testing is dependent on the scope and schedule for EIDM Release 2. QSSI is proposing to implement the open defects from Release 1 and upgrade of <b>NotRes</b> Release 2. Currently QSSI is <b>sp</b> planning to schedule performance testing for the week of 05/20/2013.</p> <p>QSSI has requested CMS a dedicated window in implementation environment to execute the performance testing. Currently with applications integrated with EIDM in implementation environment, execution of the testing and implementing the recommendations from <b>NotRe</b> product team will be very difficult and <b>sp</b> potentially impact other applications testing their applications with EIDM.</p>
2. <b>NotRes</b>	508 noncompliance issue. This week's 508 testing at CMS 508 Tab failed with only 25% score.	02/15/2013	High	Open	<p>Update on 07/21/2013: We are still testing the 508 issues in the test environment.</p> <p>Update on 07/14/2013: QSSI EIDM will be implementing the workarounds provided by <b>NOTRES</b> for the 508 issues in the Test</p>

					<p>Environment as part of our scheduled deployment on tuesday 07/16/2013</p> <p>Update on 07/07/2013: No further updates.</p> <p>Update on 06/30/2013: We have escalated the issues to Sev 1 and are working with</p> <p>Update on 06/23/2012: QSSI still working with on the issue.</p> <p>Update on 06/16/2012: QSSI is working with the team this week to further troubleshoot the issue and identify possible fix for the same.</p> <p>Update on 06/10/2012: No further updates.</p> <p>Update on 06/10/2012: No further updates.</p> <p>Update on 5/3/2013: Out of 4 defects fixed, only one defect has passed 508 testing. QSSI will setup a meeting with to perform further troubleshooting.</p> <p>Updated on 04/29/2013: 4 defects addressed and resolved in the Test Environment. Remaining 7 defects are still under analysis with QSSI EIDM and Product team.</p> <p>QSSI has submitted a remediation plan for resolving the 508 defects. There are in all 11 defects and all 11 defects have SR opened with product development team for analysis and resolution.</p>	
3	NotResp	replication issue in the EIDM Test Environment and a one-off issue related new tcp connection. Analysis indicates that this is a known issue and a hot fix will be provided by to resolve this issue. This issue does not exist in Implementation environment, since production environment is similar to the implementation environment – the issue will not affect EIDM in production.	03/12/2013	Low	Open	<p>This issue occurs only in test environment because there is only instance. Awaiting patch from to fix the issue in Test Environment.</p>
4.		Standalone WaaS Database configuration and development is not	3/14/2013	Medium	Open	<p>Update on 07/21/2013: We are still testing the</p>

complete. This issue does not affect the current HIOS application integration. This will only impact for those applications that will need retrieval of data from the WaaS Database.				<p>web service in the lower environments. We will close the issue once we have successfully tested the same in all the environments.</p> <p>Update on 07/14/2013: Issue will be closed once the WaaS DB configuration is successfully tested in the Test environment.</p> <p>Update on 07/07/2013: This task has been completed and deployed in the Test environment.</p> <p>QSSI has completed 75% of code development and will be ready to implement for Release 3. Awaiting CMS confirmation on Release 3 scope.</p>
<p>5. <b>NotResp</b> IP address change affects implementation of <b>NotResp</b> EIDM User Registration process. At the time, we created the rules for google recaptcha, the set of public IPs were different.</p> <p><b>NotResp</b></p> <p><b>NotResp</b> URL is pointing to another pool.</p> <p><b>NotResp</b> this pool actually belongs to google.com. <b>NotResp</b> is being set up as an alias (we believe this is a very recent change).</p>	03/16/2013	Medium	Open	<p>Update on 07/21/2013: No further updates.</p> <p>Update on 07/14/2013: No further updates.</p> <p>Update on 07/07/2013: No further updates.</p> <p>Update on 06/30/2013: No further updates.</p> <p>Update on 06/23/2013: No further updates.</p> <p>Update on 06/16/2013: No further updates.</p> <p>Update on 06/10/2013: This is pending on CMS decision on OAAM. This will be a non-issue if we proceed with OAAM implementation.</p> <p>Update on 5/17/2013: Awaiting CMS Response to the proposed options.</p> <p>Update on 05/13/2013: Alternative options for implementing CAPTCHA sent to CMS on 05/13/2013. Additional time was taken to analyze the option of using <b>NotResp</b> as of the solution for implementing CAPTCHA to prevent BOT attacks.</p> <p>Update on 05/03/2013: Discussed options for <b>NotResp</b> QSSI to send the write-up on the preferred solution on 05/06/2013. CMS EIDM will analyze the solution and provide approval</p>

				to proceed further. <b>NotResp</b> will be removed from Release 1 Increment 2. Alternate suggestions for implementing a solution to prevent BOT attacks have been provided to CMS. Additional meeting will be scheduled this week and the timeline for alternate implementation for <b>NotResp</b> will be provided to CMS by this week.
6. EIDM ARS integration issue. Currently the EIDM application solution to step up users from LOA 1 to LOA 3 for users who have undergone manual identity proofing is not working. The issue is related to receiving and processing the response from Experian ARS web service.	3/26/2013	High  <b>Tracking  Purposes: Affects  finalizing Release  #3 scope and  schedule</b>	Open	Update on 07/21/2013: We are still testing the web service in the lower environments. We will close the issue once we have successfully tested the same in all the environments. Update on 07/14/2013: Issue will be closed once QSSI EIDM team successfully tests the ARS web services in all the environments. Update on 07/07/2013: No further updates. Update on 06/30/2013: ARS webservices were deployed in the Test environment on 06/25/2013. Currently going through system testing. Update on 06/23/2013: No further updates. Update on 06/16/2013: QSSI is working on the new WSDL for the ARS calls. Update on 06/10/2013: It was decided with CMS on 06/07/2013 to have a new WSDL for the ARS calls. Update on 06/02/2013: QSSI reached out to SAIC to request for additional information on the Analytics Augmented ID proofing method. Update on 05/03/2013: Awaiting CMS decision on Experian's Augment Analytics approach. On HOLD – due to emergency changes implemented to default LOA #1 for users registering through New User Registration link

				in CMS Portal.
7. Decision on Identity proofing users and determination of LOA 2 , LOA 3 is awaited from CMS. As per Email sent to CMS OIS team by Henry Chao on 04/23/2013, there might be a change in the RIDP decisioning strategy to make the RIDP process simpler.	4/22/2013	High  <b>Tracking Purposes: Affects finalizing Release #3 scope and schedule</b>	Open	<p>Update on 07/21/2013: The OOW questions list was shared by CMS to SAIC. SAIC shared the sub codes to QSSI EIDM team on 07/19/2013, QSSI EIDM team will implement the new sub codes in the lower environment.</p> <p>Update on 07/14/2013: The OOW questions list was shared by CMS to SAIC. SAIC plans to implement the sub codes by 07/28/2013, following which EIDM team will implement the same in the lower environment.</p> <p>Update on 07/07/2013: Meeting with SAIC was held on Tuesday 7/2. QSSI still awaiting the sub codes. CMS has made the decision to use Analytics Augmented approach for both LOA 2 and LOA 3. CMS will be sending the CMS approved OOW questions list to SAIC for them to implement the strategy and provide the sub codes.</p> <p>Update on 06/30/2013: QSSI is still awaiting the Sub Codes from SAIC. QSSI to set up a meeting with SAIC &amp; CMS to get the latest updates on Id Proofing and plan for next steps.</p> <p>Update on 06/23/2013: QSSI is awaiting CMS to finalize the questions provided by SAIC.</p> <p>Update on 06/16/2013: No further updates.</p> <p>Update on 06/10/2013: It was decided with CMS on 06/07/2013 to proceed with Augmented Analytics approach for LOA2 ID Proofing. Pending decision on the use of Augmented Analytics for LOA3 Id proofing. Until further direction from CMS it was decided to follow the existing Id Proofing process for LOA3.</p> <p>Update on 06/02/2013: Still awaiting CMS</p>

						<p>decision on the approach</p> <p>Update on 05/03/2013: Awaiting CMS decision on Experian's Augment Analytics approach.</p> <p>QSSI is currently using the web services provided by SAIC/Experian to Id Proof and user at LOA 2 and LOA 3. Any change to the decisioning strategy will require rework for the web services and the user interface developed so far in EIDM to Identity Proof a user.</p>
8. Installation of Active-Active Solution	NotResp	n CMS BDC to support EIDM	05/03/2013	Medium	Open	<p>Update on 07/21/2013: NotResp confirmed that they will provide the fix for the patch on the week of July 29th 2013. We are also working on fixing the NotResp functional issue on URL direct. It is being tracked as a Sev1 SR. We have additional issues that were identified while installing the NotResp components in the BDC environment.</p> <p>1. BDC environment was set up with non NotResp system accounts, security constraints with the EDCG do not allow any NotResp components to be installed with NotResp system account names. For the NotResp active active solution to work, NotResp will have to be installed with the NotResp system accounts.</p> <p>2. The BDC environment is not in Sync with the Terremark environment with OS versions. Both the conditions listed above are required for the NotResp active active solution to work.</p> <p>Update on 07/14/2013: It was decided to install all the NotResp components in BDC exactly similar to what we currently have in the Terremark Production environment. QSSI EIDM team has shared the installation CD with the BDC team for the initial scan. Two OCS resources from QSSI EIDM team will be on site at the BDC location for the installation</p>

				<p>of <b>NotResp</b> components on Monday.</p> <p>Update on 07/07/2013: Installation of <b>NotResp</b> continues to be on hold since the issues identified with <b>NotResp</b> have not been resolved yet. Delivery of patch for <b>NotResp</b> active active solution from <b>NotResp</b> is TBD, this was earlier scheduled to be 07/15/2013. QSSI has submitted a document listing the current issues and options impacting release 3 with <b>NotResp</b> to CMS.</p> <p>Update on 06/30/2013: QSSI has installed the <b>NotResp</b> database with the required schemas, followed by <b>NotResp</b>. QSSI plans to install <b>NotResp</b> and Installation of <b>NotResp</b> is on hold until the <b>NotResp</b> issue is resolved.</p> <p>Update on 06/23/2013: QSSI had multiple meetings with the CMS EDC team to review the design and more meetings are scheduled for this week.</p> <p>Update on 06/16/2013: QSSI has provided the CMS EDC team with the updated EIDM diagrams. QSSI technical team also participated in a meeting with CMS EDC to further discuss the global load balancer requirements and how they can be configured. Additionally, the <b>NotResp</b> was successfully installed and tested in the Test environment.</p> <p>Update on 06/10/2013: URS and TM are in the process of implementing the firewall rules post CMS approval.</p> <p>Update on 06/02/2013: QSSI is awaiting the firewall rules to be implemented between TerreMark and BDC. Additionally, <b>NotResp</b> support has added a requirement to install the <b>NotResp</b> before it is installed and configured in BDC. QSSI would require</p>
--	--	--	--	--



				<p>additional 5 weeks to apply the patch in the TM lower environments and perform regression testing.</p> <p>Update on 5/24/2013: QSSI has successfully installed and configured the DB and replication is on hold until a firewall between TerreMark and BDC is opened. Once replication is configured, installation and configuration will commence followed by installations.</p> <p>Update on 05/17/2013: QSSI started supporting installation of BDC from 5/16/2013. Only one work station is provided to QSSI for installation, which will delay the process of setting up in Test, Validation and Production Environment.</p> <p>Update on 05/03/2013: Awaiting decision from CMS on whether QSSI is required to install or to provide expertise to CMS BDC to install and configure at BDC.</p>
<p>9. Scope for Release 3 is not finalized. QSSI is working on completing the requirements and development of web services. Requirements for web services are expected to complete 5/10 and development of web services will be complete on 5/17/2013. QSSI will need CMS help for finalizing the following:</p> <ul style="list-style-type: none"> <li>Additional details related to integration of Agents, Brokers and Navigators – QSSI has forwarded the proposed workflow (initial) to CMS on 04/29/2013 and will respond to Venkat's response by 5/6/2013.</li> <li>Decision on Experian Augmented Analytics to step up a user LOA to LOA # 2 and LOA #3.</li> <li>Infrastructure and Network connectivity between CSR and FFM application is not finalized or at least QSSI is not aware when FFM and CSR applications will be integrated in Test Environment. QSSI needs the integrated environment to configure the federation of CSR users.</li> </ul>	5/3/2013	<p>High</p> <p><b>Tracking Purposes: Affects finalizing Release #3 scope and schedule.</b></p>	Open	<p>Update on 07/21/2013: QSSI EIDM has shared the updated integrated schedule with all application integration schedules included on 07/21/2013.</p> <p>Update on 07/14/2013: QSSI EIDM has shared the integrated schedule with CMS on 07/12/2013.</p> <p>Update on 07/07/2013: QSSI submitted the draft version of the schedule to CMS, QSSI will submit the completed version for CMS review by Friday 07/12/2013.</p> <p>Update on 06/30/2013: QSSI provided a draft version of the schedule and will continue to work on the schedule.</p> <p>Update on 06/23/2013: QSSI to provide an high level schedule to CMS this week.</p>



<ul style="list-style-type: none"> <li>Integration requirements from SHOP, PAS Applications.</li> </ul> <p>Note: This issue is affecting finalizing the release schedule for integrating EIDM with CSR, Consumer Portal and SHOP.</p>				<p>Update on 06/16/2013: QSSI is still working on the new schedule and will provide an updated schedule on the basis of the recent developments.</p> <p>Update on 06/10/2013: QSSI had a meeting with CMS on 06/07/2013 and most of the items were finalized. QSSI will provide CMS with the updated schedule based on the decisions made in the meeting.</p> <p>Updates on 06/02/2013: High level plan with an integrated schedule was presented to CMS on 05/30/2013. QSSI is awaiting response from CMS.</p> <p>Update on 5/24/2013: QSSI is working with Deb to come up with the complete scope for Release 3. The QSSI team is working on required LOE to come up with a schedule that will be shared with CMS by end of this week.</p> <p>Update on 5/17/2013: QSSI has completed development of web service (to use for integration between EIDM, Consumer Portal and CSR) and deployed in Test environment on 5/17/2013. Final System Requirements for web services will be sent to CMS this week.</p> <p>QSSI PM to review with CMS EIDM on the next steps and will work with CMS to finalize the schedule for Release 3.</p>
<p>10. Lack of information on testing schedule for applications integrated with EIDM. This affects QSSI ability to plan for testing activities like performance testing in EIDM Implementation Environment.</p>	5/8/2013	High	Open	<p>Update on 07/21/2013: We do have a dedicated environment for Performance testing IMPL1. The current environment built is just for <b>NOT Res</b>, we will keep this issue open till the environment is complete with all <b>NOTK esd</b> and <b>Not</b> components.</p> <p>Update on 07/14/2013: No further updates.</p> <p>Update on 07/07/2013: No further updates.</p> <p>Update on 06/30/2013: No further updates.</p>

				<p>Update on 06/23/2013: No further updates.</p> <p>Update on 06/16/2013: No further updates.</p> <p>Updates on 06/16/2013: No further updates</p> <p>Updates on 06/10/2013: No further updates</p> <p>Updates on 5/24/2013: No further updates</p> <p>Update on 5/24/2013: No additional updates. Still waiting on schedule that specifies testing activities for other applications.</p> <p>Update on 5/17/2013: Awaiting details from CMS EIDM team on the testing activities for other applications integrated with EIDM in Test and Implementation Environment.</p> <p>To discuss with CMS and request for a weekly or bi-weekly meeting within applications integrated with EIDM (a meeting similar to CCB) and request for a schedule update from respective applications on their respective application testing activities including SCA in Test and Implementation Environment.</p>
<p>11. Resolution to <b>NotRe</b> SRs opened for <b>NotRe</b> development Team. Currently there are 4 SRs opened and is expected to resolved as part of <b>NotRe</b> <b>sp</b></p>	5/6/2013	Medium	Open	<p>Update on 07/21/2013: The list of <b>NotRe</b> SR's with latest status is attached in the Risks section. <b>sp</b></p> <p>Update on 07/14/2013: The list of <b>NotRe</b> SR's with latest status is attached in the Risks section. <b>sp</b></p> <p>Update on 07/07/2013: QSSI to provide weekly status on open <b>NotRe</b> SRs to CMS. The first status report will be submitted to CMS on Monday 8th July 2013 in the format requested by CMS. <b>sp</b></p> <p>Update on 06/30/2013: QSSI shared the entire list of <b>NotRe</b> SRs with current status to CMS. QSSI has also planned a weekly meeting with <b>NotRe</b> to review the status on each SR. <b>sp</b></p>

				<p>Updates on 06/23/2013: No further updates.</p> <p>Updates on 06/16/2013: No further updates.</p> <p>Updates on 06/10/2013: No further updates.</p> <p>Updates on 5/24/2013: No further updates.</p> <p>Update on 5/17/2013: Hot fix from [NotRe] is awaited this week for resolving 4 SRS. As per OCS [NotRe] does not contain any fix that will be useful for EIDM, expecting [NotRe] to be released in Mid-June and that is expected to provide resolution to some performance issues.</p> <p>QSSI is working with [NotRe] development team to find out when [NotRe] will be ready for EIDM. Response from [NotRe] is awaited.</p>
12. Migration of EIDM Data Layer [NotRe] and Database) from Virtual to Physical machines.	5/17/2013	High	Open	<p>Update on 07/21/2013: No further updates.</p> <p>Update on 07/14/2013: No further updates.</p> <p>Update on 07/07/2013: No further updates.</p> <p>Updates on 06/30/2013: No further updates.</p> <p>Updates on 06/23/2013: No further updates.</p> <p>Updates on 06/16/2013: No further updates.</p> <p>Updates on 06/10/2013: No further updates.</p> <p>Update on 5/24/2013: Meeting on 5/23/2013 was postponed due to unavailability of key contributors to this discussion. This meeting will be scheduled for some time this week.</p> <p>Update on 05/17/2013: QSSI/OCS to provide the sizing of [NotRe] and Database layer to TerreMark on 5/21/2013. Meeting scheduled for 5/23/2013 to discuss the requirements and next steps on migration tasks related to migration of EIDM to Physical machines.</p>
13. [NotResp] Active-Active solution does not support Asynchronous deployment. The Baltimore Data Center hosts the CMS Portal, but not FFM or other consumer facing applications which are only	5/17/2013	High	Open	<p>Update on 07/21/2013: [NotRe] has confirmed that the patch will be ready on the week of July 29<sup>th</sup> 2013. QSSI is continuing with installation of all other components in the BDC</p>

hosted at Terremark. In OAM terms, this is referred to an "asynchronous" deployment.				<p>environment.</p> <p>Update on 07/14/2013: No further updates.</p> <p>Update on 07/07/2013: No further updates.</p> <p>Updates on 06/30/2013: No further updates.</p> <p>Update on 06/23/2013: QSSI awaiting input from Oracle to submit the white paper.</p> <p>Updates on 06/16/2013: QSSI is reviewing the document with <del>Notre</del> and will provide the white paper this week.</p> <p>Updates on 06/10/2013: QSSI will send the white paper this week with <del>Notre</del> recommendation and follow it up with a meeting.</p> <p>QSSI will send a white paper on the current status and will schedule a meeting with CMS to discuss the next steps on the deployment of Active-Active solution at BDC.</p>
14. Currently, EIDM is performing all the tasks of getting the approvals and doing all the paper work for environment change requests by external application owners, the work is labor intensive and would need better process considering the number of applications integrating with EIDM is increasing.	06/21/2013	Low	Open	<p>Update on 07/21/2013: No further updates.</p> <p>Update on 07/14/2013: No further updates.</p> <p>Update on 07/07/2013: CMS EIDM team directed QSSI not to initiate any application integration meeting unless QSSI has approval from the CMS EIDM GTL.</p> <p>Updates on 06/30/2013: No further updates.</p> <p>Issue was discussed with CMS in the last status meeting and CMS would have an internal meeting to identify the right process. Future use of Remedy by application owners was suggested by QSSI.</p>
15. Lack of information on the MLN data source for Agent/Broker application could impact the Production deployment date of August 11 <sup>th</sup> 2013	07/20/2013	High	Open	<p>Update on 07/21/2013: The issue has been escalated to the CMS EIDM team, QSSI EIDM team has configured the application in the test environment with a dummy table for testing purposes.</p> <p>Getting all the firewall rules implemented for</p>

<p>16. Delay in setup of EIDM Development Environment. This has become a serious issue as most of the defects identified in the test environment could not be detected in the current EIDM Development environment hosted in TerreMark Federal cloud. The current Development environment is not a completely integrated environment with <b>NotResp</b> and SOA components and with increasing complexity of EIDM solution, the EIDM Development environment currently used is not helping identify issues before deploying into Test environment</p>	<p>03/14/2013</p>	<p>High   <b>Tracking  Purposes: Affects  troubleshooting  and analysis of  defects for  Release 2  (Schedule #4 and  #6) and Release 3.</b></p>	<p>Closed</p>	<p>the MLN data validation across all the environments could be a challenge.</p> <p>Update on 07/21/2013: The set up of the development environment is now complete.</p> <p>Update on 07/14/2013: The customization of EIDM application was delayed with resources assigned to other high priority activities including the Performance Testing effort. The scheduled completion of Dev environment is now 07/18/2013.</p> <p>Update on 07/07/2013: The base installation of the Development environment was completed on 07/05/2013. Further customization of EIDM application will be completed by 07/12/2013. There were some delays due to firewall implementation.</p> <p>Update on 06/30/2013: No Further updates.</p> <p>Update on 06/23/2013: With the current status QSSI tentatively estimates the completion of the Dev Environment by 07/08/2013.</p> <p>Update on 06/16/2013: No further updates.</p> <p>Update on 06/10/2013: Some of the resources were pulled for other high priority tasks which impacted the development of the Dev Environment. With the current status QSSI estimates the completion of the Dev Environment by 06/24/2013.</p> <p>Update on 05/17/2013: QSSI resumed building of Dev Environment from 5/16/2013. We are estimating to complete the setup of dev environment to be complete by 6/17/2013.</p> <p>Update on 05/10/2013: QSSI was told by URS that the operating system were downgraded by URS but QSSI still could not verify and proceed with building the Dev Environment. QSSI has opened a ticket and assigned it to</p>
--	-------------------	--	---------------	--

				<p>URS.</p> <p>Update on 05/03/2013: QSSI reported Operating System mismatch with the VM delivered by URS. Since EIDM is implemented with <b>NotResp</b> in Test, Implementation and Production – QSSI prefers URS deliver VMs for development environment with the same version.</p>
--	--	--	--	---

Risks	DATE OPENED	PROBABILITY / IMPACT	STATUS	CONTINGENCY PLAN
<p>1. If <b>NotResp</b> products defects are not addressed in the timely manner, then EIDM implementation schedule and quality of the solution will be negatively impacted.</p>	08/23/2012	Low/High	Active	<p>Update on 07/21/2013: The list of all open <b>NotResp</b> SRs is attached with the latest current status on each SR.</p> <p><b>NotResp</b></p> <p>Update on 07/14/2013: The list of all open <b>NotResp</b> SRs is attached with the latest current status on each SR.</p> <p>Update on 07/07/2013: QSSI EIDM team to work with CMS to finalize plan on <b>NotResp</b> QSSI EIDM will provide weekly report on all open <b>NotResp</b> SRs to CMS.</p> <p>Updates on 06/30/2013: On further testing of <b>NotResp</b> QSSI testing team found some functionality with URL redirect not working as expected. <b>NotResp</b> development team has advised QSSI EIDM team to install <b>NotResp</b> to fix the issue. The development is also working on fixing the issue with <b>NotResp</b> to avoid the <b>NotResp</b> install. Since <b>NotResp</b> is a big installation and may impact other EIDM deployments, QSSI is working very closely with <b>NotResp</b> for alternate arrangements. A decision will have to be made early next week with the help of CMS for next steps.</p> <p>Update on 06/23/2013: QSSI team continues to work with the <b>NotResp</b> team to fix the issues.</p>



				<p>Updates on 06/16/2013: QSSI team is actively working with the Product and Engineering team to analyze and fix the issues. <b>NotResp</b> upgrade Patch of <b>NotR</b> was successfully installed in the lower environments.</p> <p>The Project Team has established a weekly touch point with the Product Team to discuss open issues. <b>NotResp</b> Senior Management for Product Development has committed to providing immediate support on any issues identified by the EIDM Project Team.</p>
2. <b>NotResp</b> cannot be configured in Terremark VM.	10/18/2012	Low/Medium	Active	<p>Update on 07/21/2013: No further updates.</p> <p>Update on 07/14/2013: No further updates.</p> <p>Update on 07/07/2013: No further updates.</p> <p>Update on 06/30/2013: No further updates.</p> <p>Update on 06/23/2013: QSSI system Engineers had visted the Culpeper facility and inventoried available hardware in May 2013. All relevant information were captured (CPU, RAM etc). Storage used to host <b>NotRe</b> DB VMs is still under discussion between QSSI <b>NotRe</b> and <b>NotRe</b>. Various options were visited. QSSI is waiting on direction from CMS.</p> <p>Updates on 06/16/2013: No Further updates.</p> <p>Received Email from Peter Um that TM will support physical storage. QSSI has provided the requested EIDM Specifications for physical storage to Peter Um on 12/07/2012.</p> <p>As an alternative to ensuring High Availability, QSSI and Oracle recommend configuring <b>NotRe</b> DB with <b>NotResp</b> and for EIDM Release 1 – this will be the option that will be implemented. At this time the issue does not prevent proceeding forward for EIDM Release #1, but QSSI will further discuss and provide a plan for implementing <b>NotResp</b> post EIDM Release #1.</p>
3. Decision on Disaster Recovery Strategy and site for CMS Private Cloud is not determined.	10/22/2012	Medium/High	Active	<p>Update on 07/21/2013: No further updates.</p> <p>Update on 07/14/2013: No further updates.</p> <p>Update on 07/07/2013: No further updates.</p> <p>Update on 06/30/2013: No further updates.</p>

				<p>Update on 06/23/2013: No further updates.</p> <p>Update on 06/16/2013: No further updates.</p> <p>Updates on 06/16/2013: No Further updates.</p> <p>As per Email from Doug Margush on 10/24/2012, the decision is still pending with CMS.</p> <p>As per Email received from Thomas Schankweiler on 11/12/2012, the suggestion is track this as an issue till this is solved.</p> <div>NotResp</div>
--	--	--	--	--



# Health Insurance Marketplace Pre-Flight Checklist

---

## Health Insurance Marketplace IT Systems

**Centers for Medicare & Medicaid Services**

**September 17, 2013**

Updated: 9/17/13

Template Version 5 (template updated on 9/13/2013)





## Table of Contents

End-to-End Scenarios Checklist.....	3
Functionality Checklist.....	4
Interface Checklist.....	14
Non Functional Development Checklist.....	17
Security Checklist .....	18
Security activities .....	18
Security Operations.....	18
Section 508 Compliance.....	19
Data Preparation Checklist .....	19
Performance & Stress Testing Checklist .....	20
Scenario: Register new accounts .....	20
Scenario: User completes the application .....	20
Scenario: Key hub interfaces.....	21
Scenario: FFM sends 834s to Issuers .....	21
Scenario: Issuers send 834s to FFM .....	22
Elasticity & Scalability Checklist .....	22
Environments and Infrastructure Checklist .....	23
Environments.....	23
Architecture .....	25
Agreements Checklist .....	28
Issuer Checklist.....	29



Agent/Broker Checklist .....	29
State Checklist.....	29
Federal Checklist.....	33
Operations Checklist .....	34
Confirm escalation path.....	34
Help Desk and Support Operations Readiness .....	35
Points of Contact.....	35
Triage Team and Tool Checklist .....	35
Monitoring Checklist .....	36
Production Control and Monitoring .....	37
Documentation Checklist.....	37

## End-to-End Scenarios Checklist

Goals:

- Confirm that key end-to-end scenarios have been demonstrated and proven to work

#	Scenario	Demonstrated successfully?
1	A QHP eligible consumer registers on healthcare.gov and completes a non-financial assistance application	
2	A QHP eligible consumer registers on healthcare.gov and completes a financial assistance application	
3	A Medicaid/CHIP eligible consumer completes an application	

General Criteria	Scenario Specific Criteria	
------------------	----------------------------	--



Obtained via FOIA by Judicial Watch, Inc.

<ul style="list-style-type: none"> <li><input type="checkbox"/> User is able to navigate to the learn site on HC.gov</li> <li><input type="checkbox"/> LOA1 account created</li> <li><input type="checkbox"/> Identity proofing and LOA2 step up successful</li> <li><input type="checkbox"/> Correct application questions and cards are displayed</li> <li><input type="checkbox"/> Verification calls through the hub are correct</li> <li><input type="checkbox"/> Plan compare filtering and navigation is correct</li> <li><input type="checkbox"/> Premiums display correctly</li> <li><input type="checkbox"/> User can select a plan and receive instructions on premium payment (premium redirect or billing from issuer)</li> <li><input type="checkbox"/> 834 generation (syntax and content) is successful (FFM creates XML for Hub and Hub generates correct 834)</li> <li><input type="checkbox"/> Correct notices are generated</li> <li><input type="checkbox"/> Expected user experience features are in place</li> <li><input type="checkbox"/> Appropriate metrics are available through MIDAS</li> <li><input type="checkbox"/> Interface calls are confirmed in the logs (e.g., FFM to Hub; FFM/Hub to MIDAS; Hub to external partners)</li> <li><input type="checkbox"/> Inspect database for successful insertion of records</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Scenario #1 scenario (A QHP eligible consumer registers on healthcare.gov and completes a non-financial assistance application) <ul style="list-style-type: none"> <li><input type="radio"/> Income related questions are not displayed</li> <li><input type="radio"/> Eligibility determination for QHP is correct</li> </ul> </li> <li><input type="checkbox"/> Scenario #2 scenario (A QHP eligible consumer registers on healthcare.gov and completes a financial assistance application) <ul style="list-style-type: none"> <li><input type="radio"/> Income related questions are displayed</li> <li><input type="radio"/> Eligibility determination for QHP is correct</li> <li><input type="radio"/> APTC calculation is correct</li> <li><input type="radio"/> Premium displays with the APTC reduction displayed clearly</li> </ul> </li> <li><input type="checkbox"/> Scenario #3 scenario (A Medicaid/CHIP eligible consumer completes an application) <ul style="list-style-type: none"> <li><input type="radio"/> Eligibility determination for Medicaid/CHIP is correct</li> </ul> </li> </ul>
---	---

## Functionality Checklist

### Goals:

- Confirm that functional development is completed
- Identify incomplete development
- Describe known problems so that operations is prepared

### Change Log

Date	Notes
9/11/13 (10:00 PM)	CGI updates to FFM column.
9/13/13 (5:30 PM)	Additions to Template
9/16/13 (2:25 PM)	CGI Updates in preparation for 9/16 5pm Meeting

Business Capability	Function <sup>1</sup>	Development Complete? (Y, N, N/A)							Tested successfully? <sup>2</sup>	Known Problems
		FFM	Hub	MIDAS	EIDM	NGD	Serco	HC.gov Learn		
Create Account	9/16 Items to Discuss: <ul style="list-style-type: none"> <li>Agent Broker Landing Page</li> <li>CCR Land Page</li> <li>Session Management</li> </ul>									
	Agent/Broker Landing Page	N							Not tested successfully	UI is done; Service not testing well. Service responds with inappropriate results. Working to fix component by component. Data models updated, services being worked. (Clarify UI and Service) Complete by 9/14.  9/16: Not going to go – working through various role based scenarios. Ties with CCR Landing page as well. Every time the path changes, it interferes with session based management. Every change made creates an unintended consequence elsewhere. Best Case Scenario – 2 business days away from Agent Broker and CCR Landing Pages.
	Settings: Communication Preferences	Y							Yes	
Static Page saying Change of Circumstance coming 10/15	Settings: Coverage Information - Report Life Changes	Y								
	Landing Page (Global): My Apps and Coverage Global Landing Page	Y								Critical defect, UI is not showing 'complete' status when application is done. Target no later than 9/15.  9/16: Above task completed on 9/13
	Consumer Landing Page ( Tenant)	Y							Defect #11269	Cleaning up issues on Navigation. Plans

<sup>1</sup> Functions with an asterisk (\*) were deferred from 10/1 Go-Live

<sup>2</sup> Tested successfully = (1) No high severity defects open; (2) as judged by the business and CMS management, remaining lower severity defects will not degrade consumer experience.



Business Capability	Function <sup>1</sup>	Development Complete? (Y, N, N/A)							Tested successfully? <sup>2</sup>	Known Problems
		FFM	Hub	MIDAS	EIDM	NGD	Serco	HC.gov Learn		
										and Programs not displaying properly. Defect fix target completion 9/12. Updated to be 9/13 for fix completion. Will target 9/13 build to not allow users to create multiple applications for 1 tenant.  9/16: Navigation and Plans and Programs have been cleaned up. In process of final fixes for 9/16 release.
	Settings: Premium Discount Usage – NOT DAY 1	NA								
	Authorized Rep (Day 1 Capabilities) – NOT DAY 1	NA								
	CCR Landing Page	N							No	UI Pages done; working to connect with Call Center. Need to reintegrate CCR specific services (major bug). Need to figure out how to bypass EIDM. (Best case scenario – complete by 9/14). Update – more likely to be 9/15 build.  9/16: Targeted for 9/16 release. There may be an issue with how Call Center connects with the Marketplace.
	Settings: Application Details	Y							Defect #11275	Not showing correct status, but in progress of being fixed. Defect fix target completion 9/12. Update, still an issue and targeting 9/14 build.  9/16: Defect fixes targeted for 9/16
	LOA2 - Online ID Proofing	Y								EIDM dependencies – setting up accounts for us to test with Experian. Update – still an issue on EIDM side.  CGI to coordinate with Karlton Kim on this issue.  9/16: No major problems



Business Capability	Function <sup>1</sup>	Development Complete? (Y, N, N/A)							Tested successfully? <sup>2</sup>	Known Problems
		FFM	Hub	MIDAS	EIDM	NGD	Serco	HC.gov Learn		
	LOA2 - Manual ID Proofing	Y								EIDM dependencies – setting up accounts for us to test with Experian. CGI to coordinate with Karlton Kim on this issue. FFM has critical defect to step-up account. Currently have hotfix to resolve to continue testing.  9/16: Defect under debugging – targeting 9/18 release. Venkat from OIS is talking with Experian about a Date of Birth issue that impacts testing. Testing is inconsistent due to this DOB issue.
Submitting document upload to ESD, and creating task in their queue to manage that document	LOA2 - ESD ID Proofing	Y								EIDM dependencies – setting up accounts for us to test with Experian. CGI to coordinate with Karlton Kim on this issue  9/16: Had to make some changes due to the fact that ESD won't have a Task Queue for Day 1. There needs to be a way to alert the user once a document is uploaded. Pod 5 is done with their piece to pull the ESD worker's accept/decline document decision, but Pod 4 needs to write the code that actually captures this decision.
	Message Center – NOT DAY 1 – Using Bulletin Board	NA								
	My Plans & Programs	Y								Plans okay; Working on issues with Programs and links on the page. Critical fixes targeted for 9/13 and 9/14.  9/16: Went in on 9/15, still doing some clean-up on it today.
	Settings: Terminate Coverage	Y								Only the Terminate enrollment/policy is scheduled for 9/15 build; other items are in testing.  9/16: Target for 9/16 release.



Business Capability	Function <sup>1</sup>	Development Complete? (Y, N, N/A)							Tested successfully? <sup>2</sup>	Known Problems
		FFM	Hub	MIDAS	EIDM	NGD	Serco	HC.gov Learn		
	ToDo List	Y							Yes	Linking over to the Plan Compare ToDo List for Day1. 9/16: This is done.
	Settings: Authorized Users (Day 1 = Agent/Brokers)	Y								Moving in parallel with Agent/Broker Landing Page task for 9/14 build. 9/16: Above task completed on 9/13
	Direct Enrollment Issuer Entry Page	Y								
	Inconsistencies List	N								Working on simplified version – targeting 9/15 build; potential ESD dependency.  9/12: Dependency on the Eligibility Results PDF from Pod 1. This won't be totally complete until Pod 1 finishes the Eligibility Results PDF.  9/16: Had to make some changes due to the fact that ESD won't have a Task Queue for Day 1. There needs to be a way to alert the user once a document is uploaded. Pod 5 is done with their piece to pull the ESD worker's accept/decline document decision, but Pod 4 needs to write the code that actually captures this decision. Needs more testing.
	My Profile Page	Y							Test complete	
	Settings: Eligibility Results and Appeals	N								Dependency on Pod 1 to replicate and links to PDF (9/15)  9/16: Still waiting for 1 final piece of PDF to be completed from Pod 1.
	Notices (Dev complete for Day 1 notices except Eligibility Results which is scheduled for 9/15)	Y							Can be tested in Prod Prime now.	Update – able to see notice generate and display on bulletin board.





Business Capability	Function <sup>1</sup>	Development Complete? (Y, N, N/A)							Tested successfully? <sup>2</sup>	Known Problems
		FFM	Hub	MIDAS	EIDM	NGD	Serco	HC.gov Learn		
Application	<p>9/16/13: Items to Discuss</p> <ul style="list-style-type: none"> <li>ESC Mec Card</li> <li>FIPS Code for POD1 targeting 9/17 - Get logic or screen shots on how it will work, should be home address and not mailing address</li> <li>Eligibility Results (test out entire process down to Gluster and then out to EFT) - Has EFT been setup for mail contractor?</li> <li>PCR not working (1) residesTogether is not getting set in member association in write in child scenario (UI); (2) but also not getting set when the residesWithIndicator is set when the parent and child are both applicants.</li> <li>Did not see the Did not agree with attestation to give Medicaid Agency right to pursue question, but child found ineligible because did not attest to yes to this attestation. IMPACT is that for the people who should have this attestation the system is denying Medicaid because it is using the default value of false.</li> <li>SLCSP calculation is incorrectly incorporating an individual who is marked as ineligible for APTC (appropriately) because he/she has Medicare. NotResp (prod) included a spouse w/o Medicare, and NotResp (prod) flipped the spouse to Medicare. SLCSP and max APTC were identical for both.</li> </ul>									
	Household Contact	Y								<p>Observation: confirmed that EIDM is passing the CamelCase information. Clarify with Pod 5 to see how this is being saved in My Account (EIDM Value or User-Entered Value).</p> <p>9/16: CamelCase is coming from a system of record, so decided not to do any data manipulation of it for 10/1.</p>
	Attestations	N								
	My Account Integration	Y								
	Security and Other UI Changes	Y								
	Additional Information	Y							Needs Integration Testing	ESC MEC Integration not complete - target 9/12



Business Capability	Function <sup>1</sup>	Development Complete? (Y, N, N/A)							Tested successfully? <sup>2</sup>	Known Problems
		FFM	Hub	MIDAS	EIDM	NGD	Serco	HC.gov Learn		
										9/16: Did not make it into 9/12; new target release for 9/16
	Delayed Response	Y							Needs Integration Testing	Pages developed; Integration with service is broken. Fix in progress – target 9/12. 9/16: Fixed on 9/12
	Capture Assistor Identification	Y								-Security questions need to be promoted to Test2 9/16: Done
	Eligibility Results	N								PDF Page still in progress. UI is done, PDF is in progress. Working with Adobe. Target 9/15. 9/16: Most of the work is done; 1 piece left to finish (Integration with ESC-MEC)
	Income Screener related to Help Paying for Coverage	Y								
	Building the Household & Personal Information	Y							Known defects, in process of being fixed	Working the critical defects - targeting as many as possible for 9/12 (can refer to Defect Tracker/list for defect details) 9/16: Many defects have been closed, but some still remain in open and are in progress.
	Special Circumstances	Y								
	Household Summary	Y								
	Income	Y							Known defects, in process of being fixed	Several defects identified – working through the list and targeting for 9/12. 9/16: Fixed several Income defects with 9/16 target
	SEP Questions (Not for 10/1)	Y							Known defects in SEP cards – code in Dev2 should have the fixes in place. Fixes will be checked in by 9/12.	Development is done, but deferred until 11/1.



Business Capability	Function <sup>1</sup>	Development Complete? (Y, N, N/A)							Tested successfully? <sup>2</sup>	Known Problems
		FFM	Hub	MIDAS	EIDM	NGD	Serco	HC.gov Learn		
	Review Application	Y							2 Defects on Review Screen (Download)	Targeting 9/12 for defect fixes
	Sign and Submit	Y								Has an integration point with Attestation questions. Integration is still missing - target 9/12. 9/16: Done.
	Get Started	Y							One defect identified, it's been fixed and in Dev2, will move to Test2 on 9/12.	
	* Household Contact ID Proofing (not for 10/1)	NA								
	* Second Chance (not for 10/1)	NA								
Eligibility Determination										
	Verify Non-ESC MEC (For available data sources only).	Y	Y							Known defects, in process of being fixed. Testing on 9/11, see Eligibility High Priority Defect List.  9/12: Wasn't able to test with the existing independent set of data, but hit blockers. Now testing with a known set of data that was created in-house; allowing us to make progress in testing. Mathematica is in route, and we'll work with them to get an independent set of data to test with.
	Verify Citizenship/Lawful Presence	Y	Y							Known defects, in process of being fixed. Testing on 9/11, see Eligibility High Priority Defect List.  9/12: Wasn't able to test with the existing independent set of data, but hit blockers. Now testing with a known set of data that was created in-house; allowing us to make progress in testing. Mathematica is in route, and we'll work with them to get an independent set of



Business Capability	Function <sup>1</sup>	Development Complete? (Y, N, N/A)							Tested successfully? <sup>2</sup>	Known Problems
		FFM	Hub	MIDAS	EIDM	NGD	Serco	HC.gov Learn		
										data to test with. 9/13: Verified Successfully
	Verify Incarceration	Y	Y							Known defects, in process of being fixed. Testing on 9/11, see Eligibility High Priority Defect List.  9/12: Wasn't able to test with the existing independent set of data, but hit blockers. Now testing with a known set of data that was created in-house; allowing us to make progress in testing. Mathematica is in route, and we'll work with them to get an independent set of data to test with.
	Verify SSN	Y	Y							Known defects, in process of being fixed. Testing on 9/11, see Eligibility High Priority Defect List.  9/12: Wasn't able to test with the existing independent set of data, but hit blockers. Now testing with a known set of data that was created in-house; allowing us to make progress in testing. Mathematica is in route, and we'll work with them to get an independent set of data to test with.  good
	Verify Current Income	Y	Y							Known defects, in process of being fixed. Testing on 9/11, see Eligibility High Priority Defect List.  9/12: Wasn't able to test with the existing independent set of data, but hit blockers. Now testing with a known set of data that was created in-house; allowing us to make progress in testing.



Business Capability	Function <sup>1</sup>	Development Complete? (Y, N, N/A)							Tested successfully? <sup>2</sup>	Known Problems
		FFM	Hub	MIDAS	EIDM	NGD	Serco	HC.gov Learn		
										Mathmatica is in route, and we'll work with them to get an independent set of data to test with.  good
	Predetermination processing	Y								Known defects, in process of being fixed. Testing on 9/11, see Eligibility High Priority Defect List.  9/12: Wasn't able to test with the existing independent set of data, but hit blockers. Now testing with a known set of data that was created in-house; allowing us to make progress in testing. Mathmatica is in route, and we'll work with them to get an independent set of data to test with.
	Process attestations	Y								Known defects, in process of being fixed. Testing on 9/11, see Eligibility High Priority Defect List.  9/12: Wasn't able to test with the existing independent set of data, but hit blockers. Now testing with a known set of data that was created in-house; allowing us to make progress in testing. Mathmatica is in route, and we'll work with them to get an independent set of data to test with.
	Qualify for enrollment period	Y								Known defects, in process of being fixed. Testing on 9/11, see Eligibility High Priority Defect List.  9/12: Wasn't able to test with the existing independent set of data, but hit



Business Capability	Function <sup>1</sup>	Development Complete? (Y, N, N/A)							Tested successfully? <sup>2</sup>	Known Problems
		FFM	Hub	MIDAS	EIDM	NGD	Serco	HC.gov Learn		
										blockers. Now testing with a known set of data that was created in-house; allowing us to make progress in testing. Mathematica is in route, and we'll work with them to get an independent set of data to test with. 9/12: Wasn't able to test with the existing independent set of data, but hit blockers. Now testing with a known set of data that was created in-house; allowing us to make progress in testing. Mathematica is in route, and we'll work with them to get an independent set of data to test with.
	Manage Insurance Application and Determine Individual Eligibility	Y								Known defects, in process of being fixed. Testing on 9/11, see Eligibility High Priority Defect List.  9/12: Wasn't able to test with the existing independent set of data, but hit blockers. Now testing with a known set of data that was created in-house; allowing us to make progress in testing. Mathematica is in route, and we'll work with them to get an independent set of data to test with.
	Determine Residency eligibility	Y								Known defects, in process of being fixed. Testing on 9/11, see Eligibility High Priority Defect List.  9/12: Wasn't able to test with the existing independent set of data, but hit blockers. Now testing with a known set of data that was created in-house; allowing us to make progress in testing. Mathematica is in route, and we'll work



Business Capability	Function <sup>1</sup>	Development Complete? (Y, N, N/A)							Tested successfully? <sup>2</sup>	Known Problems
		FFM	Hub	MIDAS	EIDM	NGD	Serco	HC.gov Learn		
	Determine Indian Status	Y								<p>with them to get an independent set of data to test with.</p> <p>Known defects, in process of being fixed. Testing on 9/11, see Eligibility High Priority Defect List.</p> <p>9/12: Wasn't able to test with the existing independent set of data, but hit blockers. Now testing with a known set of data that was created in-house; allowing us to make progress in testing. Mathematica is in route, and we'll work with them to get an independent set of data to test with.</p>
	Determine QHP Eligibility	Y								<p>Known defects, in process of being fixed. Testing on 9/11, see Eligibility High Priority Defect List.</p> <p>9/12: Wasn't able to test with the existing independent set of data, but hit blockers. Now testing with a known set of data that was created in-house; allowing us to make progress in testing. Mathematica is in route, and we'll work with them to get an independent set of data to test with.</p>
	APTC/CSR Eligibility	Y								<p>Known defects, in process of being fixed. Testing on 9/11, see Eligibility High Priority Defect List.</p> <p>High Priority Defect: Possibly a problem that's it not selecting second lowest cost plan. We have a test scenario that will expose this problem.</p>



Business Capability	Function <sup>1</sup>	Development Complete? (Y, N, N/A)							Tested successfully? <sup>2</sup>	Known Problems
		FFM	Hub	MIDAS	EIDM	NGD	Serco	HC.gov Learn		
	Determine Medicaid/CHIP Eligibility	Y								<p>Known defects, in process of being fixed. Testing on 9/11, see Eligibility High Priority Defect List.</p> <p>Magi 3 rule verification – still need to validate (it was being skipped for many people).</p> <p>9/12: Wasn't able to test with the existing independent set of data, but hit blockers. Now testing with a known set of data that was created in-house; allowing us to make progress in testing. Mathematica is in route, and we'll work with them to get an independent set of data to test with.</p>
	Household Composition	Y								<p>Known defects, in process of being fixed. Testing on 9/11, see Eligibility High Priority Defect List.</p> <p>9/12: Wasn't able to test with the existing independent set of data, but hit blockers. Now testing with a known set of data that was created in-house; allowing us to make progress in testing. Mathematica is in route, and we'll work with them to get an independent set of data to test with.</p>
	Complete eligibility	Y								<p>Known defects, in process of being fixed. Testing on 9/11, see Eligibility High Priority Defect List.</p> <p>9/12: Wasn't able to test with the</p>





Business Capability	Function <sup>1</sup>	Development Complete? (Y, N, N/A)							Tested successfully? <sup>2</sup>	Known Problems
		FFM	Hub	MIDAS	EIDM	NGD	Serco	HC.gov Learn		
										existing independent set of data, but hit blockers. Now testing with a known set of data that was created in-house; allowing us to make progress in testing. Mathematica is in route, and we'll work with them to get an independent set of data to test with.
	Start Clocks	Y								Known defects, in process of being fixed. Testing on 9/11, see Eligibility High Priority Defect List.  9/12: Wasn't able to test with the existing independent set of data, but hit blockers. Now testing with a known set of data that was created in-house; allowing us to make progress in testing. Mathematica is in route, and we'll work with them to get an independent set of data to test with.
Plan Compare	9/16 Items to Discuss • Take out security (need to verify with CMS) • BRMS Error									
	Premium redirect	Y							Yes	Submit a BRF request and turn the flag off to return to the issuers site. – Completed 9/12 and will verify by 9/13.  9/16: Turned on in Prod Prime but not in Test2 yet. Will be in Test2 on 9/16 (evening).
	Anonymous Shopper	Y							Yes	Defects identified by CMS, being treated as critical, target fixes for 9/12  9/12: Mark Oh: Don't focus on Anonymous Shopper first – turn focus to Plan Compare instead.



Business Capability	Function <sup>1</sup>	Development Complete? (Y, N, N/A)							Tested successfully? <sup>2</sup>	Known Problems
		FFM	Hub	MIDAS	EIDM	NGD	Serco	HC.gov Learn		
										9/16: No change
	Calculate Max APTC	Y							Yes	9/16: Working a defect that is truncating decimal points for premium amounts.
	To Do List	Y							Yes	
	* Elect APTC amount - Multi-tax household (not for 10/1)	NA							Yes	
	* Plan Select- Multi-tax Filer Household (not for 10/1)	NA							Yes	
	* Change of Circumstances (not for 10/1)	NA							Yes	
	Compose Enrollment Groups	Y							Yes	
	Screening Questions	Y							Yes	
	Elect APTC amount - single household	Y							Yes	Related to Max APTC, Defects identified by CMS, being treated as critical, target fixes for 9/12. Known issue with EHB Calculation to get Max APTC (Plan Management defect).  Defects identified by CMS, being treated as critical, target fixes for 9/12 and 9/13.  9/16: Fixed all critical defects (9/15 evening)
	* Elect APTC amount - Multi-member household(not for 10/1)	NA							Yes	
	Plan Results	Y							Yes	
	Plan Details	Y							Yes	
	Compare Plans	Y							Yes	Internal defects identified, fixed completed on for 9/12 build, currently verifying.  9/16: No critical defects
	Save Plans	Y							Yes	



Business Capability	Function <sup>1</sup>	Development Complete? (Y, N, N/A)							Tested successfully? <sup>2</sup>	Known Problems
		FFM	Hub	MIDAS	EIDM	NGD	Serco	HC.gov Learn		
	Retrieve Plans	Y							Yes	
	Plan Select- Single Household	Y							Yes	
	* Plan Select- Multi-Member Household (not for 10/1)	NA								
Direct Enrollment										
	Secure Redirect	Y							Yes	CMS working on workaround with Issuers for .NET technologies.  9/16: Still open. Check with Mark Oh for target?
	Fetch Eligibility	Y							Yes	Fixed defects, include in 9/12 release. Critical defect being analyzed which is getting NULL pointer exception.  9/16: Defects fixed on 9/15
	Submit Enrollment - Create	Y							Yes	Waiting for new service that has more validations. Existing code will be replaced with more validation services. Target for 9/13 build. Rounding logic issue for premium amounts – address with issuers by 9/15.  9/16: Pod 1 needs to do modeling changes (FIPS). Trying to unit test code changes.
	Submit Enrollment – Change (not for 10/1)	NA								
	Submit Enrollment - Cancel	Y							Not tested yet – Part of new service	Waiting for new service that has more validations. Existing code will be replaced with more validation services. Target for 9/15  9/16: Pod 1 needs to do modeling changes (FIPS). Trying to unit test code changes.



Business Capability	Function <sup>1</sup>	Development Complete? (Y, N, N/A)							Tested successfully? <sup>2</sup>	Known Problems
		FFM	Hub	MIDAS	EIDM	NGD	Serco	HC.gov Learn		
	Submit Enrollment - Terminate/Disenroll	Y							Not tested yet – Part of new service	Target for 9/15 9/16: Pod 1 needs to do modeling changes (FIPS). Trying to unit test code changes.
Enrollment	9/16 Items to Discuss: Navigator/Agent (in Assister section) information is not being saved as part of the application nor being sent as part of 834.									9/16: Fixing this in the new service – targeting 9/17 build
	Initial Enrollment	Y							Currently testing	New Service targeted for 9/13 build. 9/16: Targeted for 9/17 build
	Process Inbound 834s for Effectuation, Cancellation and Termination (Disenrollment) of Enrollments from Issuers	Y							Yes (no CMS or Issuer testing yet) 9/12: Test bed exists – need to get into Prod Prime to test.	Need to have some issuers do some testing in this function. It is in Prod Prime. 9/16: No change
	Transaction Logging - 999, 824XML, 834 (Inbound and Outbound)	Y							Yes (no CMS or Issuer testing yet) 9/12: Test bed exists – need to get into Prod Prime to test.	Need to have some issuers do some testing in this function. It is in Prod Prime. Update – critical defect that does the transaction logging is not working properly. Currently analyzing for resolution. 9/16: Fixing defect for 9/16
	Process 999 Acknowledgement	Y							Yes (no CMS or Issuer testing yet) 9/12: Test bed exists – need to get into Prod Prime to test.	Need to have some issuers do some testing in this function. It is in Prod Prime. Update – critical defect identified, currently analyzing for resolution. 9/16: Fixing defect for 9/16
	Change Enrollment - Demographic Changes, Address Change, Add/Remove member (Not for 10/1 – 10/15 Target)	NA								
	Change Enrollment - Cancel/Terminate Enrollment	Y							Not tested yet	New Code is developed, Unit Testing in progress – target 9/15 release for Test2. 9/16: Targeted for 9/17 build



Business Capability	Function <sup>1</sup>	Development Complete? (Y, N, N/A)							Tested successfully? <sup>2</sup>	Known Problems
		FFM	Hub	MIDAS	EIDM	NGD	Serco	HC.gov Learn		
	Generate Outbound 834s for Initial, Change, Cancel, Terminate Enrollments	Y							Old code has been tested; new code has not been tested yet	Initial will go in 9/13 build; Change/Cancel/Terminate will go to Test2 on 9/15. 9/16: Targeted for 9/17 build
Call Center										
	Find Person/Find Authorized Rep	Y							Yes	No critical defects remain as of 9/11. Addressing serious defects. 1 Serious defect being addressed.
	Find Individual Applications	Y							Yes	No critical defects remain as of 9/11. Addressing serious defects.
	Fetch Individual Application Details	Y							Yes	No critical defects remain as of 9/11. Addressing serious defects.
	Fetch Shop Employee Details (not for 10/1 – 11/1 Target)	NA								No critical defects remain as of 9/11. Addressing serious defects.
	Fetch Activity Log	Y							Yes	No critical defects remain as of 9/11. Addressing serious defects. My Account is still working on capturing account logs
	Send Eligibility Task Escalation	Y							Yes	No critical defects remain as of 9/11. Addressing serious defects.
	Fetch Eligibility Task	Y							Yes	No critical defects remain as of 9/11. Addressing serious defects.
	Update Account	Y							Yes	No critical defects remain as of 9/11. Addressing serious defects.
	Unlock Account/Reset Forgotten Password	Y							Yes	No critical defects remain as of 9/11. Addressing serious defects.
Eligibility Case Management										
	Serco Case Management Solution									
	FFM Interfaces for Serco									
Eligibility Support Desktop										
	Custom Notice	N								UI still in progress with target of 9/15 (if



Business Capability	Function <sup>1</sup>	Development Complete? (Y, N, N/A)							Tested successfully? <sup>2</sup>	Known Problems
		FFM	Hub	MIDAS	EIDM	NGD	Serco	HC.gov Learn		
										not complete for 9/12)
	Integration With ESC	Y							Yes	
	Task Queue/Workflow	Y							Not yet – Not able to log in due to EIDM	Working open defects.
	Task Assignment to ESW	Y							Not yet – Not able to log in due to EIDM	Working open defects.
	Document Upload	Y							Not yet – Not able to log in due to EIDM	Working open defects.
	View Documents	Y							Not yet – Not able to log in due to EIDM	Working open defects.
	Task Notes	Y							Haven't been able to test in Test2 yet	No defects
	Document Management – NOT DAY 1	NA								
	Review and Adjudication of documents submitted by consumer	N								Targeting to complete by 9/12 – Issue Resolution; RIDP is at risk for 912 because Pod 5 just completed the modeling changes needed to move forward.
Reports and Metrics / Other										
	MMI Dashboard: 17 metrics			Y					No – in progress in PROD Prime	
	MMI Report: 17 metrics			Y					No – in progress in PROD Prime	
	MMI Export File: 17 metrics			Y					No – in progress in PROD Prime	
	E&E Dashboard			Y					No – in progress in PROD Prime	
	E&E Report: Saved vs. Submitted Applications (FFM)			Y					No – in progress in PROD Prime	
	E&E Report: Applicants Waiting for an Eligibility Determination (FFM)			Y					No – in progress in PROD Prime	
	E&E Report: Applicants in an Inconsistency/Good Faith Period (FFM)			Y					No – in progress in PROD Prime	
	E&E Report: Eligibility Determinations by QHP (FFM)			Y					No – in progress in PROD Prime	
	E&E Report: Eligibility Determinations/Assessments for IAPs (FFM)			Y					No – in progress in PROD Prime	



Business Capability	Function <sup>1</sup>	Development Complete? (Y, N, N/A)							Tested successfully? <sup>2</sup>	Known Problems
		FFM	Hub	MIDAS	EIDM	NGD	Serco	HC.gov Learn		
	E&E Report: Self Service Functionality			Y					No – in progress in PROD Prime	
	MIDAS: Office of Enterprise Management (OEM) extract			Y					No – in progress in PROD Prime	
	MIDAS: Health Insurance Casework System (HICS) extract			Y					No – in progress in PROD Prime	
	MMI Dashboard: 17 metrics			Y					No – in progress in PROD Prime	
	MMI Report: 17 metrics			Y					No – in progress in PROD Prime	
	MMI Export File: 17 metrics			Y					No – in progress in PROD Prime	
	E&E Dashboard			Y					No – in progress in PROD Prime	
	E&E Report: Saved vs. Submitted Applications (FFM)			Y					No – in progress in PROD Prime	
	E&E Report: Applicants Waiting for an Eligibility Determination (FFM)			Y					No – in progress in PROD Prime	
	E&E Report: Applicants in an Inconsistency/Good Faith Period (FFM)			Y					No – in progress in PROD Prime	
	E&E Report: Eligibility Determinations by QHP (FFM)			Y					No – in progress in PROD Prime	
	E&E Report: Eligibility Determinations/Assessments for IAPs (FFM)			Y					No – in progress in PROD Prime	
	E&E Report: Self Service Functionality			Y					No – in progress in PROD Prime	
	MIDAS: Office of Enterprise Management (OEM) extract			Y					No – in progress in PROD Prime	
	MIDAS: Health Insurance Casework System (HICS) extract			Y					No – in progress in PROD Prime	
	MMI Dashboard: 17 metrics			Y					No – in progress in PROD Prime	
	MMI Report: 17 metrics			Y					No – in progress in PROD Prime	
	MMI Export File: 17 metrics			Y					No – in progress in PROD Prime	
	E&E Dashboard			Y					No – in progress in PROD Prime	
	E&E Report: Saved vs. Submitted Applications (FFM)			Y					No – in progress in PROD Prime	
	E&E Report: Applicants Waiting for an Eligibility Determination (FFM)			Y					No – in progress in PROD Prime	
	E&E Report: Applicants in an Inconsistency/Good Faith Period (FFM)			Y					No – in progress in PROD Prime	



Business Capability	Function <sup>1</sup>	Development Complete? (Y, N, N/A)							Tested successfully? <sup>2</sup>	Known Problems
		FFM	Hub	MIDAS	EIDM	NGD	Serco	HC.gov Learn		
	E&E Report: Eligibility Determinations by QHP (FFM)			Y					No – in progress in PROD Prime	
	E&E Report: Eligibility Determinations/Assessments for IAPs (FFM)			Y					No – in progress in PROD Prime	
	E&E Report: Self Service Functionality			Y					No – in progress in PROD Prime	
	MIDAS: Office of Enterprise Management (OEM) extract			Y					No – in progress in PROD Prime	
	MIDAS: Health Insurance Casework System (HICS) extract			Y					No – in progress in PROD Prime	
	MMI Dashboard: 17 metrics			Y					No – in progress in PROD Prime	
	MMI Report: 17 metrics			Y					No – in progress in PROD Prime	
	MMI Export File: 17 metrics			Y					No – in progress in PROD Prime	
	E&E Dashboard			Y					No – in progress in PROD Prime	
	E&E Report: Saved vs. Submitted Applications (FFM)			Y					No – in progress in PROD Prime	
Other Services for SBMs										
	RIDP		Y							
	Federal Verifications		Y							
HC.Gov Learn Site										
	Help Content Completed									





## Interface Checklist

Goals:

- Confirm that interfaces are ready for the go-live
- Identify incomplete development
- Describe known problems so that operations is prepared

Business Capability	Interface	Infrastructure – Connectivity Established (Prod-to-Prod)? (Y, N, N/A)	Interface Complete? (Y, N, N/A)								Tested successfully? <sup>3</sup> (i.e., no high severity defects)	Known Problems	
			FFM	Hub	MIDAS	EIDM	NGD	Serco	HC.gov Learn	External Partner			
Create Account													
	FFM - EIDM		Y	N/A	N/A	Y	N/A	N/A	N/A	N/A	Full testing not complete	EIDM dependencies – setting up accounts for us to test with Experian. Testing team input: Integration testing of FFM components (E&E, FM, and PM) not testing as a whole in the same environment	
	FFM – Gov Delivery		Y	N/A	N/A	Y	N/A	N/A	N/A	N/A	Full testing not complete	Testing team input: Integration testing of FFM components (E&E, FM, and PM) not testing as a whole in the same environment	
	FFM – HC.gov		Y	N/A	N/A	Y	N/A	N/A	Y?	N/A	Full testing not complete	Testing team input: Integration testing of FFM components (E&E, FM, and PM) not testing as a whole in the same environment	
Application													
	N/A												
Eligibility													
	FFM – Hub	Y	Y	Y	N/A	N/A	N/A	N/A	N/A	N/A	Y		

<sup>3</sup> Tested successfully = (1) No high severity defects open; (2) as judged by the business and CMS management, remaining lower severity defects will not degrade consumer experience.



Business Capability	Interface	Infrastructure – Connectivity Established (Prod-to-Prod)? (Y, N, N/A)	Interface Complete? (Y, N, N/A)								Tested successfully? <sup>3</sup> (i.e., no high severity defects)	Known Problems
			FFM	Hub	MIDAS	EIDM	NGD	Serco	HC.gov Learn	External Partner		
	Hub – Account Transfer	Partial		Y		N/A	N/A	N/A	N/A	N/A	Started testing, continuing next week with remaining states	
	Hub – Experian	Y		Y		N/A	N/A	N/A	N/A	N/A	Y – SBM/RIDP testing starting today, calling EIDM service	
	Hub – MIDAS	N	N/A	Y		N/A	N/A	N/A	N/A	N/A		
	Hub – SSA	N	N/A	Y	N/A	N/A	N/A	N/A	N/A	N/A	Y –Source : DSH Schedule 9/6/2013)	
	Hub – IRS	N	N/A	Y	N/A	N/A	N/A	N/A	N/A	N/A	Y –Source : DSH Schedule 9/6/2013)	
	Hub – Equifax	N	N/A	Y	N/A	N/A	N/A	N/A	N/A	N/A	Y –Source : DSH Schedule 9/6/2013)	
	Hub – Medicare	N	N/A	Y	N/A	N/A	N/A	N/A	N/A	N/A	Y –Source : DSH Schedule 9/6/2013)	
	Hub – DHS v32.1	N	N/A	Y		N/A	N/A	N/A	N/A	N/A	Y	
	Hub – DHS v33	N	N/A	Y	N/A	N/A	N/A	N/A	N/A	N/A	Y –Source : DSH Schedule 9/6/2013)	



Business Capability	Interface	Infrastructure – Connectivity Established (Prod-to-Prod)? (Y, N, N/A)	Interface Complete? (Y, N, N/A)								Tested successfully? <sup>3</sup> (i.e., no high severity defects)	Known Problems
			FFM	Hub	MIDAS	EIDM	NGD	Serco	HC.gov Learn	External Partner		
	Hub - OPM	N	N/A	Y	N/A	N/A	N/A	N/A	N/A	N/A	Y –Source : DSH Schedule 9/6/2013)	
	Hub - TRICARE	N	N/A	Y	N/A	N/A	N/A	N/A	N/A	N/A	Y –Source : DSH Schedule 9/6/2013)	
	Hub – Peace Corps	N	N/A	Y	N/A	N/A	N/A	N/A	N/A	N/A	Y –Source : DSH Schedule 9/6/2013)	
	Hub - VA	N	N/A	Y	N/A	N/A	N/A	N/A	N/A	N/A	Y –Source : DSH Schedule 9/6/2013)	
	Hub – State Medicaid Agencies	N	N/A	Y	N/A	N/A	N/A	N/A	N/A	N/A	Y – (Source : DSH Schedule 9/6/2013)	
	FFM – Mailing Contractor		Y?	N	N/A	N/A	N/A	N/A	N/A	N/A	N – As of Daily Status Report 9/13/2013	
	HIGLAS Integration		Y?	Y	N/A	N/A	N/A	N/A	N/A	N/A	Scheduled for testing between 9/13/013 and 9/17/2013 (Source: ACA Daily Testing Report 9/12/2013)	
	FFM – Adobe LiveCycle		N	N/A	N/A	N/A	N/A	N/A	N/A	N/A	PDF Page still in progress. UI is done, PDF is in progress. Working with Adobe. Target 9/15. (Source: CGI	



Business Capability	Interface	Infrastructure – Connectivity Established (Prod-to-Prod)? (Y, N, N/A)	Interface Complete? (Y, N, N/A)								Tested successfully? <sup>3</sup> (i.e., no high severity defects)	Known Problems
			FFM	Hub	MIDAS	EIDM	NGD	Serco	HC.gov Learn	External Partner		
											Update in previous section)	
Direct Enrollment												
	FFM – Issuer (Web Services)		Y	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Partially Complete?	Waiting for new service that has more validations. Existing code will be replaced with more validation services. Target for 9/15 (Source: CGI Update in previous section)
Enrollment												
	FFM – Hub (for enrollment transactions)		Y	Y	N/A	N/A	N/A	N/A	N/A	N/A	Partially Complete?	Need to have some issuers do some testing in this function. It is in Prod Prime. (Source: CGI Update in previous section)
	Hub – Issuers (EFT/EDI for 834 transactions)		Y	Y	N/A	N/A	N/A	N/A	N/A	N/A	Y – (Source : DSH Schedule 9/6/2013)	
Call Center												
	FFM – Call Center		Y	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Y – (Source: CGI Update in previous section)	No critical defects remain as of 9/11. Addressing serious defects.
	Call Center access to FFM		Y	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Y – (Source: CGI Update in previous section)	No critical defects remain as of 9/11. Addressing serious defects.
Eligibility Support												
	ESW (Serco) Federated Access to FFM		Y?	N/A	N/A	N/A	N/A	Y?	N/A	N/A	Partially Complete? - (Source: CGI	Targeting to complete by 9/12 – Issue Resolution; RIDP is at risk for 912



Business Capability	Interface	Infrastructure – Connectivity Established (Prod-to-Prod)? (Y, N, N/A)	Interface Complete? (Y, N, N/A)								Tested successfully? <sup>3</sup> (i.e., no high severity defects)	Known Problems
			FFM	Hub	MIDAS	EIDM	NGD	Serco	HC.gov Learn	External Partner		
											Update in previous section)	
Reports and Metrics												
	MIDAS – FFM		Y?	N/A	Y?	N/A	N/A	N/A	N/A	N/A	ACA Testing scheduled for 09/13/2013-09/17/2013(Source: ACA Daily Testing Report 9/12/2013)	
	MIDAS – Hub		N/A	Y?	Y?	N/A	N/A	N/A	N/A	N/A	ACA Testing Scheduled for 09/13/2013-09/17/2013(Source: ACA Daily Testing Report 9/12/2013)	
Other Services for SBMs												
	Hub – SBM		N/A	Y	N/A	N/A	N/A	N/A	N/A	N/A	Y – (Source : DSH Schedule 9/6/2013)	
MIDAS												
	FFM to provide port information to MIDAS for the Content Pump Configuration	Y	Y		Y							
	DSH to provide port information to MIDAS for the Content Pump	Y		Y	Y							



Business Capability	Interface	Infrastructure + Connectivity Established (Prod- to-Prod)? (Y, N, N/A)	Interface Complete? (Y, N, N/A)								Tested successfully? <sup>3</sup> (ie., no high severity defects)	Known Problems
			FFM	Hub	MIDAS	EIDM	NGD	Serco	HC.gov Learn	External Partner		
	Configuration											



## Non Functional Development Checklist

Goals:

- Confirm that key non-functional development items have been addressed
- Identify incomplete development
- Describe known problems so that operations is prepared

Business Capability	FFM (Y, N, N/A)						Hub (Y, N, N/A)						MIDAS (Y, N, N/A)						Notes
	Error Handling	User Friendly Error Messaging	Logging	Browser Compatibility	Transaction Management	Caching & Memory Management	Error Handling	User Friendly Error Messaging	Logging	Browser Compatibility	Transaction Management	Caching & Memory Management	Error Handling	User Friendly Error Messaging	Logging	Browser Compatibility	Transaction Management	Caching & Memory Management	
Create Account																			
Application																			
Eligibility Determination																			
Plan Compare																			
Direct Enrollment																			
Enrollment																			
Call Center																			
Eligibility Support Desktop																			
Reports and Metrics / Other																			
Other Services for SBMs																			





## Security Checklist

### Goal

- Ensure that security activities have been completed and that operations is ready

### Security activities

System	SCA/ATO Completed? (Y, N, N/A)		High Findings Remediated? (Y, N, N/A)	Residual Risks	Notes
	SCA	ATO			
FFM	Y	Y	N	2 High, 22 moderate, 13 low risks	See certification form for details.
Hub	Y	Y	Y	19 moderate, 1 low risk;	See certification form for details.
MIDAS	Y	Y	Y	33 moderate, 32 low risk;	See certification form for details.
EIDM	Y	Y	Y	(need to research this)	
XOC	Y	N	N	(TBD)	ATO pending 10-25
Akamai					

### Security Operations

Item	Ready? (Y/N)	Notes
Security tools & monitoring configured?	N	
Staffing plan finalized?	N	24x7x365 coverage will be available by 9/20/2013
Incident response plan finished and ready?	Y	Ready, tested, and stakeholder training delivered.





## Section 508 Compliance

System	508 Compliant? (Y, N, N/A)	If NOT 508 Compliant, Waiver obtained? (Y, N, N/A)	Notes	Responsible
Healthcare.gov				Jon Booth/OC
FFM				
Hub				
MIDAS				
EIDM				

## Data Preparation Checklist

Data	Status? (Yes/No)	Notes	Responsible
MAGI rules from State Medicaid Agencies loaded and tested?			FFM team
Plan data loaded into HC.gov and tested?			OC / FFM Team
LOA1 user id's setup through Lite Account confirmed "ok"			EIDM Team / FFM Team
LOA1 accounts in "limbo" state identified and cleaned up from EIDM temp table			EIDM Team / FFM Team?
Test data cleared in production environment?			FFM Team / Hub Team / MIDAS Team
Reference data confirmed "ok"?			FFM Team / Hub Team / MIDAS Team



## Performance & Stress Testing Checklist

### Scenario: Register new accounts

Item	Description	Responsible
Scenario tested?		CMS Testing Team (Paul Donohoe / Akhtar Zaman)
Captured baseline SLAs for system's response time for all components? <input type="checkbox"/> FFM <input type="checkbox"/> Hub <input type="checkbox"/> EIDM <input type="checkbox"/> MIDAS		
What are the baseline SLAs (e.g., concurrent users, max transactions)?		
Is there a Performance & Stress Test Results artifact that includes (but is not limited to) actual response time from P&S test, whether tuning has occurred, post-tuning retest results, contingency plans for high & critical risks. Please include a link to or attach the artifact.		

### Scenario: User completes the application

Item	Description	Responsible
Scenario tested?		CMS Testing Team (Paul Donohoe / Akhtar Zaman)
Captured baseline SLAs for system's response time for all components? <input type="checkbox"/> FFM <input type="checkbox"/> Hub <input type="checkbox"/> EIDM <input type="checkbox"/> MIDAS		
What are the baseline SLAs (e.g., concurrent users, max transactions)?		
Is there a Performance & Stress Test Results artifact that includes (but is not limited to) actual response time from P&S test, whether tuning has occurred, post-tuning retest results, contingency plans for high & critical risks. Please include a link to or attach the artifact.		



### Scenario: Key hub interfaces

Item	Description	Responsible
Scenarios tested		CMS Testing Team (Paul Donohoe / Akhtar Zaman)
Captured baseline SLAs? <input type="checkbox"/> Hub-IRS <input type="checkbox"/> Hub-SSA <input type="checkbox"/> Other?		
What are the baseline SLAs (e.g., concurrent users, max transactions)?		
Is there a Performance & Stress Test Results artifact that includes (but is not limited to) actual response time from P&S test, whether tuning has occurred, post-tuning retest results, contingency plans for high & critical risks. Please include a link to or attach the artifact.		

### Scenario: FFM sends 834s to Issuers

Item	Description	Responsible
Scenario tested?		CMS Testing Team (Paul Donohoe / Akhtar Zaman)
Captured baseline SLAs for system's response time for all components? <input type="checkbox"/> FFM <input type="checkbox"/> Hub <input type="checkbox"/> EIDM <input type="checkbox"/> MIDAS		
What are the baseline SLAs (e.g., concurrent users, max transactions)?		
Is there a Performance & Stress Test Results artifact that includes (but is not limited to) actual response time from P&S test, whether tuning has occurred, post-tuning retest results, contingency plans for high & critical risks. Please include a link to or attach the artifact.		



Scenario: Issuers send 834s to FFM

Item	Description	Responsible
Scenario tested?		CMS Testing Team (Paul Donohoe / Akhtar Zaman)
Captured baseline SLAs for system's response time for all components? <input type="checkbox"/> FFM <input type="checkbox"/> Hub <input type="checkbox"/> EIDM <input type="checkbox"/> MIDAS		
What are the baseline SLAs (e.g., concurrent users, max transactions)?		
Is there a Performance & Stress Test Results artifact that includes (but is not limited to) actual response time from P&S test, whether tuning has occurred, post-tuning retest results, contingency plans for high & critical risks. Please include a link to or attach the artifact.		

Elasticity & Scalability Checklist

System	How will system scale (more VMs?, tuning?)	What will trigger the scaling (e.g., % CPU utilization)?	Who will do the scaling?	Is there a contingency plan if the scaling plan borrows capacity from another environment?	Notes
EIDM					
FFM					
Hub					
MIDAS					



## Environments and Infrastructure Checklist

### Environments

#### Environment Configuration

Item	Status (Yes/No)	Notes	Responsible
Do PROD, IMP0, TEST0, and DEV0 have same code base and ready to support production break fixes?			Doug Margush, Jack Fletcher
Do all environments have the same/aligned software configuration (e.g., Adobe LiveCycle, EIDM, etc)?			Doug Margush, Jack Fletcher
Have all overlaps / conflicts in environments and scheduled releases been resolved?			Doug Margush, Jack Fletcher
Are our PROD and IMP environments connected to the right Trusted Data Source (TDS) environments?			Doug Margush, Jack Fletcher, Walt
Test harness deactivated properly?			Doug Margush, Jack Fletcher, Walt Dill
DR Site ready?			Brandon Williams
DR Test conducted and validated?			Brandon Williams



Code Release Version

Environment		Proper Code Version Installed? (Yes/No and List Code Version)			Notes
	FFM	DSH	MIDAS	HC.gov Learn Site	
Responsible	FFM Team	Hub Team	MIDAS Team	HC.gov	
DEV3					
DEV2					
DEV1					
DEV0					
TEST3					
TEST2					
TEST1					
TEST0					
IMP 1A					
IMP 1B					
IMP0					
PROD					

## Architecture

Zones	Completed/Ready? (Yes/No)	Notes	Responsible
<b>Presentation Zone Configured</b>			
Intended VMs configured and ready			Doug Margush, Jack Fletcher
Web Server			Doug Margush, Jack Fletcher
Load Balance Configured			Doug Margush, Jack Fletcher
Clustering Configured			Doug Margush, Jack Fletcher
Akamai Configured – (only Akamai servers should be able to communicate with presentation zone.			Doug Margush, Jack Fletcher
<b>Application Zone Configured</b>			Doug Margush, Jack Fletcher
Intended VMs configured and ready			Doug Margush, Jack Fletcher
Adobe Live Cycle			Doug Margush, Jack Fletcher
NotResp			Doug Margush, Jack Fletcher
NotResp			Doug Margush, Jack Fletcher
Layer 7			Doug Margush, Jack Fletcher
Load Balance Configured			Doug Margush, Jack Fletcher

Zones	Completed/Ready? (Yes/No)	Notes	Responsible
Clustering Configured			Doug Margush, Jack Fletcher
NotResp Application Zone Components			Doug Margush, Jack Fletcher
Other			Doug Margush, Jack Fletcher
<b>Data Zone Configured</b>			Doug Margush, Jack Fletcher
Intended VMs configured and ready			Doug Margush, Jack Fletcher
NotResp			Doug Margush, Jack Fletcher
			Doug Margush, Jack Fletcher
			Doug Margush, Jack Fletcher
			Doug Margush, Jack Fletcher
			Doug Margush, Jack Fletcher
			Doug Margush, Jack Fletcher
			Doug Margush, Jack Fletcher
			Doug Margush, Jack Fletcher
			Doug Margush, Jack Fletcher
Other			Doug Margush, Jack Fletcher





Zones	Completed/Ready? (Yes/No)	Notes	Responsible
Other			Doug Margush, Jack Fletcher
SSL Certificates			Doug Margush, Jack Fletcher
Firewalls Configured?			Doug Margush, Jack Fletcher
SSH keys (Public & Private) properly configured?			Doug Margush, Jack Fletcher
NotResp Configured?			Doug Margush, Jack Fletcher
Program accounts removed?			Doug Margush, Jack Fletcher
Named user accounts removed?			Doug Margush, Jack Fletcher
Application logging consolidated across systems?			Doug Margush, Jack Fletcher



## Agreements Checklist

Agency	CMA Finished? (Yes/No)	SLA Finished? (Yes/No)	ISA Finished? (Yes/No)	ATC Granted? (Yes/No)	Notes	Responsible
<b>IRS</b>	CMA – Yes; Interagency Exchange Agreement (IEA)- No	Yes	Yes	Yes	<b>IRS CMA:</b> Passed the 30 day waiting period in Fed Register without issue. <b>IRS IEA:</b> IRS is the only federal partner who requires an IEA with CMS. IRS made last-minute changes to the IEA, and OGC has concerns with such. CMS is currently in discussions with IRS on the IEA changes	Daniel Lazenby, Reba Cole, Nancy Keates
<b>SSA</b>	Yes	Yes	Yes	Yes		Daniel Lazenby, Reba Cole, Nancy Keates
<b>DHS</b>	Pending	No	CMS expected to receive by 09/16/2013	Pending review and approval	<b>DHS CMA:</b> In 30-day Federal Register Waiting period until 09/19; <b>DHS SLA:</b> DHS has pushed back on transactions per minute, which they had promised to the WH. DHS cites their primary concerns as unknown TPS volume and response times; move to a new data center and service bus; etc. However, on DHS' public website, they continue to post that their TPS are in the 3- 5 minute range.	Daniel Lazenby, Reba Cole, Nancy Keates
<b>VHA</b>	Yes	No –	On 09/13, 2013, CMS received VA's Master ISA and Associate ISA. Received VA	Pending review and approval	<b>VA SLA:</b> SLA concerns are primarily with unknown TPS volume and response times. VA needed and requested metrics from testing to be reviewed prior to utilizing such as a basis	Daniel Lazenby, Reba Cole, Nancy Keates



Agency	CMA Finished? (Yes/No)	SLA Finished? (Yes/No)	ISA Finished? (Yes/No)	ATC Granted? (Yes/No)	Notes	Responsible
			signature pages for both ISA's on 09/11/2013.		for their SLA, however such metrics were not tracked during CMS' testing with VA.	
<b>DOD – Tricare</b>	Yes	No	Pending –	Pending ISA outcome	<b>DMDC SLA:</b> SLA concerns are primarily with unknown TPS volume and response times. DMDC needs and requested metrics from testing to be reviewed prior to utilizing such as a basis for their SLA. However they have recently commented that they will not know volume or TPS until Day 1 transactions come through. <b>DMDC ISA:</b> CMS provided an updated Master ISA to DMDC to review and approve, and CMS awaiting response from DMDC. DMDC had provided prior comments to the Master ISA, because they follow DOD security regulations, and not NIST security publications.	Daniel Lazenby (SLA only), Reba Cole, Nancy Keates
<b>OPM</b>	<b>DUA</b> completed	Yes	N/A	Is this required?	<b>OPM</b> has a DUA with CMS and does not need an ISA;	Daniel Lazenby (SLA only), Reba Cole, Nancy Keates
<b>Peace Corp</b>	<b>DUA</b> completed	No	N/A	Is this required?	<b>Peace Corps</b> has a DUA with CMS and does not need an ISA; <b>Peace Corps SLA:</b> primarily due to concerns regarding unknown TPS volume and response times. They are going to be routinely transferring a file to CMS.	Daniel Lazenby (SLA only), Reba Cole, Nancy Keates



Agency	CMA Finished? (Yes/No)	SLA Finished? (Yes/No)	ISA Finished? (Yes/No)	ATC Granted? (Yes/No)	Notes	Responsible
<b>Non-Fed</b>	Is this required?	Yes – 06/2013	Is this required?		<b>Equifax:</b> Non-Federal Trusted Data Source.	Daniel Lazenby (SLA only), Reba Cole, Nancy Keates
<b>Third Parties</b>						Daniel Lazenby (SLA only), Reba Cole, Nancy Keates

#### Milestones

Agency	ISA	ATC	CMA	SLA
<b>IRS</b>	09/03/2013	09/27/2013	09/15/2013	4/12/2013
<b>SSA</b>	09/03/2013	09/27/2013	09/08/2013	8/22/2013
<b>DHS</b>	09/03/2013	09/27/2013	09/20/2013	9/20/2013
<b>VHA</b>	09/03/2013	09/27/2013	09/15/2013	9/15/2013
<b>DOD –Tricare</b>	09/03/2013	09/27/2013	09/03/2013	12/27/2013
<b>Peace Corps</b>	09/03/2013	09/27/2013		
<b>OPM</b>	09/03/2013	09/27/2013		
<b>Non-Fed</b>	05/24/2013	09/27/2013		
<b>Third Parties</b>	05/24/2013	09/27/2013		

#### Issuer Checklist

Item	Status (Yes/No)	Notes	Responsible
All web services onboarding completed?			Walt Dill, Ari Knausenberger
All EDI/EFT onboarding completed?			Walt Dill, Ari Knausenberger
All Trading Partner agreements signed?			Walt Dill, Ari Knausenberger

#### Agent/Broker Checklist

Item	Status (Yes/No)	Notes	Responsible
Agent/Broker Agreements Signed?			Bing Chao
Agents/Brokers registered in EIDM?			Bing Chao
Agents/Brokers on boarded to web services API?			Bing Chao



## State Checklist

State	Connectivity			EFT Setup?	EDI Setup?	Responsible
	w/3rd Party Cert	Network	Application			
District of Columbia (DC)	Yes	Yes	Yes	Yes	Yes	Walt Dill
Hawaii (HI)	Yes	Yes	Yes	Yes	Yes	Walt Dill
Minnesota (MN)	Yes	Yes	Yes	Yes	Yes	Walt Dill
Rhode Island (RI)	Yes	Yes	Yes	Yes	Yes	Walt Dill
Vermont (VT)	Yes	Yes	Yes	Yes	Yes	Walt Dill
Colorado (CO) HCPF	Yes			Yes	Yes	Walt Dill
Colorado (CO) C4HCO	Yes	Yes	Yes	Yes	Yes	Walt Dill
California (CA)	Yes			Open	Open	Walt Dill
Connecticut (CT)	Yes	Yes	Yes	Yes	Yes	Walt Dill
Kentucky (KY)	Yes	Yes	Yes	Yes	Yes	Walt Dill
Maryland (MD)	Yes			Yes	Yes	Walt Dill
Massachusetts (MA)	Yes	Yes	Yes	Yes	Yes	Walt Dill
Nevada (NV)	Yes	Yes	Yes	Yes	Yes	Walt Dill
New York (NY)	Yes	Yes	Yes	Yes	Yes	Walt Dill
Oregon (OR)	Yes			Yes	Yes	Walt Dill
Washington (WA)	Yes	Yes	Yes	Yes	Yes	Walt Dill

Obtained via FOIA by Judicial Watch, Inc.

SBM



	State	Connectivity			EFT Setup?	EDI Setup?	Responsible
SPM	Arkansas (AR)	Yes			N/A	N/A	Walt Dill
	Delaware (DE)	Yes			N/A	N/A	Walt Dill
	New Mexico (NM)				N/A	N/A	Walt Dill
	Iowa (IA)	Yes			N/A	N/A	Walt Dill
	Michigan (MI)	Yes	Yes	Yes	N/A	N/A	Walt Dill
	Nebraska (NE)	Yes	Yes	Yes	N/A	N/A	Walt Dill
	Ohio (OH)	Yes			N/A	N/A	Walt Dill
	Idaho (ID)	Yes			N/A	N/A	Walt Dill
	Illinois (IL)	Yes			N/A	N/A	Walt Dill
	Maine (ME)				N/A	N/A	Walt Dill
	New Hampshire (NH)	Yes	Yes	Yes	N/A	N/A	Walt Dill
	South Dakota (SD)	Yes	Yes	Yes	N/A	N/A	Walt Dill
	West Virginia (WV)	Yes	Yes	Yes	N/A	N/A	Walt Dill
	Virginia (VA)				N/A	N/A	Walt Dill
	Kansas (KS)	Yes			N/A	N/A	Walt Dill
	Montana (MT)	Yes	Yes	Yes	N/A	N/A	Walt Dill
	Utah (UT)	Yes	Yes	Yes	N/A	N/A	Walt Dill
FFM	Arizona (AZ)	Yes	Yes	Yes	N/A	N/A	Walt Dill



State	Connectivity			EFT Setup?	EDI Setup?	Responsible
Alaska (AK)				N/A	N/A	Walt Dill
Florida (FL)				N/A	N/A	Walt Dill
New Jersey (NJ)	Yes			N/A	N/A	Walt Dill
Pennsylvania (PA)	Yes			N/A	N/A	Walt Dill
Missouri (MO)				N/A	N/A	Walt Dill
Wyoming (WY)				N/A	N/A	Walt Dill
Wisconsin (WI)				N/A	N/A	Walt Dill
Mississippi (MS)	Yes	Yes	Yes	N/A	N/A	Walt Dill
Oklahoma (OK)	Yes	Yes	Yes	N/A	N/A	Walt Dill
Texas (TX)	Yes			N/A	N/A	Walt Dill
Georgia (GA)	Yes	Yes	Yes	N/A	N/A	Walt Dill
North Dakota (ND)	Yes	Yes	Yes	N/A	N/A	Walt Dill
North Carolina (NC)	Yes			N/A	N/A	Walt Dill
Tennessee (TN)	Yes			N/A	N/A	Walt Dill
South Carolina (SC)	Yes			N/A	N/A	Walt Dill
Louisiana (LA)	Yes			N/A	N/A	Walt Dill
Alabama (AL)	Yes			N/A	N/A	Walt Dill
Indiana (IN)	Yes	Yes	Yes	N/A	N/A	Walt Dill



This space intentionally left blank.





### Federal Checklist

Item	Status (Yes/No)	Notes	Responsible
Connectivity established to IRS production environment?		Requires receipt of the IRS Safeguard Approval Letter prior to connection	Walt Dill / Tom Schwankweiler / Richard Speights
Connectivity established to SSA production environment?			Walt Dill / Richard Speights
Connectivity established to DHS production environment?			Walt Dill / Richard Speights
Connectivity established to VA production environment?			Walt Dill / Richard Speights
Connectivity established to DoD - TRICARE production environment?			Walt Dill / Richard Speights
Connectivity established to Peace Corps production environment?			Walt Dill / Richard Speights
Connectivity established to OPM production environment?			Walt Dill / Richard Speights



## Operations Checklist

### Confirm escalation path

Scenario	Tier 1	Tier 2	Tier 3
Consumer has a general problem or question	OC Call Center	XOSC Help Desk	Depending on issue: <ul style="list-style-type: none"> <li>Development contractors <ul style="list-style-type: none"> <li>CGI: FFM</li> <li>QSSI: Hub</li> <li>IDL: MIDAS</li> </ul> </li> <li>Technology vendors <ul style="list-style-type: none"> <li>Verizon Terremark</li> <li>Software vendor</li> </ul> </li> </ul>
Consumer needs assistance with eligibility issue	OC Call Center	Eligibility Support Worker	Depending on issue: <ul style="list-style-type: none"> <li>CMS Staff</li> <li>Development contractors <ul style="list-style-type: none"> <li>CGI: FFM</li> <li>QSSI: Hub</li> </ul> </li> </ul>
Issuer or Federal Agency calls with a problem or question	XOSC Help Desk	E& E FM LMI CGI QSSI CCIIO	Depending on issue: <ul style="list-style-type: none"> <li>CMS Staff</li> <li>Development contractors (CGI, QSSI)</li> <li>Policy (CCIIO, LMI)</li> </ul>
State calls with a problem or question	XOSC Help Desk	QSSI Regional Technical Support (RTS)	Depending on issue: <ul style="list-style-type: none"> <li>Development contractors <ul style="list-style-type: none"> <li>CGI: FFM</li> <li>QSSI: Hub</li> <li>IDL: MIDAS</li> </ul> </li> </ul>
Agent/Broker calls with a problem or question	Password Reset (XOSC)	No other help desk support	Depending on issue: <ul style="list-style-type: none"> <li>CMS Staff</li> <li>Development contractors (CGI, QSSI)</li> <li>Policy (CCIIO, LMI)</li> </ul>
XOC monitoring detects a systems issue (capacity, performance, etc)	XOC Operations Staff	Development contractors <ul style="list-style-type: none"> <li>CGI: FFM</li> <li>QSSI: Hub</li> <li>IDL: MIDAS</li> </ul>	Technology vendors <ul style="list-style-type: none"> <li>Verizon Terremark</li> <li>Software vendor</li> </ul>



### Help Desk and Support Operations Readiness

Help Desk	Scripts documented and reviewed with staff? (Yes/No)	FTE Capacity Appropriate? (normal and surge capacity) (Yes/No)	SLA Established? (Yes/No)	Informed of known problems?	Hours of Operation	Identify underlying documents	Notes
XOSC Help Desk							
EIDM Help Desk							
Experian Help Desk							
CMS IT Service Help Desk							
CGI Tier 3 Support (FFM)							
QSSI Tier 3 Support (Hub)							
CACI Tier 3 Support (MIDAS)							
OC Consumer Help Desk							

### Points of Contact

Area	Clear CMS Points of Contact Identified? (Yes/No)	If appropriate, clear external Points of Contact identified? (Yes/No)
Issuers	Yes	
Agents/Brokers	Yes	
State Based Marketplaces	Yes	
State Medicaid/CHIP Agencies		
Federal Agencies	Yes	
Trusted Data Sources (OPM, PeaceCorps, etc...)	Yes	

### Triage Team and Tool Checklist

Item	Yes/No	Notes
Remedy queues configured properly?	Yes	
Remedy reports ready?		
Do all staff have proper access to Remedy?		
Is the Triage process ready for Open Enrollment?		



Is the Triage Team staffed properly?		
--------------------------------------	--	--

## Monitoring Checklist

### Business process monitoring

Business process	Are metrics identified for monitoring (e.g., login success % for consumers)? (Yes/No)	Relevant systems						Has responsibility been assigned for monitoring the metrics? (Yes/No)	Threshold identified for the metrics? (i.e., when is there a problem to communicate? (Yes/No)	Notes
		FFM	Hub	MIDAS	EIDM	HV.gov	NGD			
Create Account										
Application										
Eligibility Determination										
Plan Compare										
Direct Enrollment										
Enrollment										

### System monitoring

System / Service	Metrics established for monitoring the system? (Yes/No)	Responsibility assigned for monitoring metrics? (Yes/No)	Threshold identified for the metrics (i.e., when is there a problem to communicate)? (Yes/No)	Notes
EIDM				
FFM				
DSH				
MIDAS				
Terremark Infrastructure (e.g., CPU utilization)	Yes	Yes	Yes	
Akamai				
Serts/Service	Yes	Yes	Yes	
EFT (Tibco)	Yes	Yes	Yes	
TWS	Yes	Yes	Yes	

### Production Control and Monitoring

Item	Yes/No	Notes
Backup configured properly?		
Backup / restore function tested and validated?		
Other relevant jobs scheduled in TWS?		
XOC monitoring tools configured?	Yes	
Contractors have procedures and instructions on what to do based on monitoring tool output?	Yes	

### Documentation Checklist

Item	Completed (Y/N)				
	FFM	Hub	MIDAS		
O&M Manual Updated					
Build/Release Notes					
Implementation tasks/plan					



---

Rollback/Backout plan					
Final defect report					
Schedule Changes (TWS) documentation					



**DRAFT:**  
**Federal Interagency Test Plan**  
**Open Enrollment 2013**

**Affordable Care Act (ACA)**

**Social Security Administration (SSA)**

**Draft V0.7.1**

**May 2, 2013**

**DISCLAIMER:** This document contains information not releasable to the public, unless authorized by law. This information has not been publicly disclosed and may be privileged and confidential. This document is intended for **Centers for Medicare & Medicaid Services (CMS)** use and distribution only and must not be disseminated, distributed, or copied to persons (or organizational entities) not authorized to receive the information. Unauthorized disclosure may result in prosecution to the full extent of the law.

## Approvals

Signature approval for the **Federal Interagency Test Plan** will be stored in the Affordable Care Act (ACA) Implementation and Testing repository. The approvers for the **Federal Interagency Test Plan** are:

**Prepared by:**

_____ <b>Sheila Burke</b> Interagency Test Technical Manager, CMS	_____ Date
---	---------------

**Prepared by:**

_____ <b>Richard Speights</b> Interagency Test Coordinator, CMS	_____ Date
---	---------------

**Prepared by:**

_____ <b>Paul Donohoe</b> Interagency Test Technical Advisor, CMS	_____ Date
---	---------------

**Reviewed by:**

_____ <b>Daniel Lazenby</b> Interagency Development Technical Advisor, CMS	_____ Date
--	---------------

**Approved by:**

_____ <b>Monique Outerbridge</b> Deputy Group Director, CMS	_____ Date
---	---------------

**Approved by:**

_____ <b>Mark Oh</b> Senior Development Technical Advisor, CMS	_____ Date
--	---------------



## Revision History

The **Revision History** provides a record of all Versions, Revisions, and Change Effective Dates of this document, the **Interagency Test Plan (“Test Plan”)**:

Change Number	Description of Change	Change Effective Date	Change Entered By
0.1	<i>Draft</i>	September 2012	CMS
0.2	<i>Draft</i>	October 14, 2012	CMS
0.3	<i>Draft</i>	October 15, 2012	CMS
0.4	<i>Draft</i>	October 16, 2012	CMS
0.5	<i>Draft</i>	October 17, 2012	CMS
0.6	<i>Draft</i>	January 03, 2013	CMS
0.6.5	<i>Draft</i>	April 3, 2013	CMS
0.7	<i>Draft</i>	May 01, 2013	CMS
0.7.1	<i>Draft</i>	May 02, 2013	CMS

# Table of Contents

1	Introduction.....	5
1.1	Overview and Scope.....	5
1.2	Audience.....	5
1.3	Document Maintenance.....	5
2	Federal Partner Profile.....	6
2.1	Federal Partner Testing Overview.....	6
2.2	Roles and Responsibilities (Federal Leads).....	6
2.3	Test Type Profile.....	7
2.3.1	Secure Communications (SC).....	7
2.3.2	FMPS-and-Partner (FP).....	7
2.3.3	Performance Stress Test (PST).....	7
2.3.4	End-to-End (E2E) / Regression Test (RT).....	8
2.3.5	Production Readiness (PR).....	8
2.4	Test Environment Profile.....	8
2.4.1	Test Environment Operations and Scheduling.....	9
2.4.2	Test Environment Security.....	9
3	Testing Process.....	10
3.1	Roles and Responsibilities (All Leads).....	10
3.2	Test Readiness.....	10
3.2.1	Interface Control Document (ICD) / Business Service Description (BSD).....	10
3.2.2	Test Readiness Checkpoint (TRC).....	10
3.2.3	Test Readiness Review (TRR).....	10
3.3	Test Tools.....	11
3.4	Test Validation.....	11
3.5	Test Reporting.....	11
4	Additional Processes.....	12
4.1	Error Handling Testing.....	12
4.2	Issue / Defect Management.....	12
4.2.1	Defect Management Workflow.....	12
4.2.2	Tracking Issues / Defects.....	13
4.2.3	Testing and Retesting Issues / Defects.....	13
4.3	Change Control (CC).....	13
5	Test Data, Scenarios, and Cases.....	15
5.1	Test Approach.....	15
5.2	Test Data, Scenarios, and Cases.....	15
5.2.1	Test Data Development.....	16
5.2.2	Test Data Deployment.....	17
5.3	Test Execution.....	17
Appendix A	Acronyms.....	19
Appendix B	Test Readiness Checkpoint (TRC) and Test Readiness Review (TRR).....	20
Appendix C	Attachment 1: Theoretical Required Root Test Cases.....	23
Appendix D	Attachment 2 – Application Creation Process.....	24
Appendix E	Attachment 3: TDS Verification Models.....	29
Appendix F	Attachment 4: Application and Payload Characteristics.....	33
Appendix G	Additional Notes.....	35

# 1 Introduction

The Patient Protection and Affordable Care Act 2010 (hereafter simply the ‘Affordable Care Act’ or ‘ACA’) mandates the establishment of Health Insurance Marketplaces (HIM) and the Federal Marketplace Program System (FMPS).

The Centers for Medicare & Medicaid Services (CMS) and Social Security Administration (SSA) will jointly participate in Interagency Testing in order to ensure the system functionality and interoperability required to support the implementation of the Federally-Facilitated Marketplace (FFM).

CMS has identified the need for a structured **Test Plan** – individualized for each Federal Agency – to guide the consistent execution of major Test activities.

## 1.1 Overview and Scope

The purpose of this document, the **Federal Interagency Test Plan ("Test Plan")**, is to outline the major Test activities agreed upon by CMS and SSA in order to support the establishment of the Federally-Facilitated Marketplace (FFM).

This document includes prescriptive how-to steps, checklists, operating procedures, and tactical guidance unique to SSA, and is organized into the following sections:

- **Section 1** – Introduction
- **Section 2** – Federal Partner Profile
- **Section 3** – Testing Process
- **Section 4** – Additional Processes
- **Section 5** – Test Data, Scenarios, and Cases
- **Appendices**

## 1.2 Audience

This document is intended for use by the executive leadership, personnel, and contractors/subcontractors of CMS and SSA.

## 1.3 Document Maintenance

CMS is responsible for maintaining the contents of this **Test Plan**, and will place each major version under Configuration Management (CM). Major revisions to this document, moreover, will require the written approval of the key *Stakeholders* identified in the **Approvals** section of this document.

## 2 Federal Partner Profile

This **Section** is organized into to following Sub-Sections:

- Federal Partner Testing Overview
- Roles and Responsibilities (Federal Leads)
- Testing Scope Profile
- Test Environment Profile

Each subject will be discussed in more detail in the following **Sub-Sections**:

### 2.1 Federal Partner Testing Overview

Each Federal Agency plays a critical role in providing the essential systems, services and verifications needed to support the establishment of the Federally-Facilitated Marketplace (FFM):

- **Centers for Medicare and Medicaid Services (CMS) / Enterprise Eligibility Service (EES):** CMS Medicare EES is the identified Trusted Data Source (TDS) for verifying an individual's Medicare Part A eligibility, which is considered a form of Minimum Essential Coverage (MEC) under the ACA.
- **Social Security Administration (SSA):** SSA is the identified TDS for verifying basic applicant information to determine enrollment and eligibility in the Marketplace, Medicaid, Children's Health Insurance Program (CHIP), and Basic Health Plan (BHP) insurance affordability programs.
- **Internal Revenue Service (IRS):** IRS is the TDS for verifying Adjusted Gross Income (AGI) and Modified Adjusted Gross Income (MAGI) information to assess if an applicant falls within the income threshold to qualify for Marketplace benefits.
- **Department of Homeland Security (DHS):** DHS is the identified TDS for information related to immigration status for alien or naturalized citizen applicants.
- **Veterans Health Administration (VHA):** VHA is the identified TDS to verify presence of health benefit coverage for VHA members.
- **Peace Corps:** Peace Corps is the identified TDS to verify presence of health benefit coverage for Peace Corps volunteers.
- **Office of Personnel Management (OPM):** OPM is the identified TDS to verify presence of health benefit coverage through the Federal Employees Health Benefits Program (FEHB Program) for the majority, but not all, Federal Agencies.
- **TRICARE:** TRICARE is the identified TDS to verify presence of health benefit coverage for TRICARE beneficiaries.
- **Equifax:** Equifax is the identified TDS for information related to Third Party income verification.

SSA's two-phased approach for Development/Testing includes:

- **Phase I:**
  - Verification of the Social Security Number (SSN), Name, and Date of Birth (DOB)
  - Confirmation of citizenship attestation
  - Indication of death
- **Phase II:**
  - Phase I processing
  - Title II Monthly Benefit information
  - Title II Annual Benefit information
  - Incarceration data
  - Quarters of Coverage information

### 2.2 Roles and Responsibilities (Federal Leads)

Well-defined roles and responsibilities; ongoing collaboration and coordination; and clear communication paths are critical for the success of Interagency Testing efforts. CMS and SSA will find it necessary to coordinate and collaborate on a variety of activities that include, but are not limited to:

- Finalizing Test Schedules
- Meeting pre-requisite Test Readiness requirements
- Keeping Test Environments operational
- Developing and deploying Test Data and Scenarios
- Providing necessary levels of database administration and technical support

The following **Table** identifies the Federal Leads from both CMS and SSA:

**Table 1: Roles and Responsibilities (Federal Leads)**

Role(s)	Partner Lead(s)
<b>CMS Lead(s)</b>	Test Manager(s)
	Test Coordinator(s)
	Test Technical Advisor(s)
	Development Technical Advisor(s)
	Test Executive(s)
<b>SSA Lead(s)</b>	
	Sheila Burke (CMS)
	Richard Speights (CMS)
	Paul Donohoe (CMS / CIISG)
	Daniel Lazenby (CMS / CIISG)
	Mark Oh (CMS / CIISG)
	Monique Outerbridge (CMS / CIISG)
	Mark Wicker (SSA)
	Pat Berlin (SSA)

## 2.3 Test Type Profile

CMS and SSA will jointly participate in the execution of several required Test Types. The following **Table** captures the high-level Testing schedule (by Test Type) for SSA:

**Table 2: High-Level Testing Schedule (Current as of April 26, 2013)**

Key Dates						
	Test Type					Production Readiness (PR)
	Secure Communication (SC)	FMPS-and-Partner (FP)	Performance Stress Test (PST)		End-to-End (E2E)	
			Fed Hub PST	FFM UI PST	Regression Test (RT)	
SSA	IMP1B 5/8 – 5/14 (Network) 5/15 – 5/31 (Application)	6/3 – 6/14	6/17 – 6/28	8/13 – 8/30	Regression Test (RT) 8/6 – 8/12	9/2 – 9/20
	IMP1A 7/16 – 7/22 (Network) 7/23 – 8/5 (Application)				End-to-End (E2E) 8/20 – 8/30	

### 2.3.1 Secure Communications (SC)

Secure Communication Testing verifies whether both CMS and SSA have the communication ports/protocols open for subsequent Test Types.

Secure Communication Testing will involve three variations of Testing:

- **Type 1:** Basic ‘Ping’ Test at the Port layer.
- **Type 2:** Certificate/Key Exchange Test at the Transport (or Network) layer.
- **Type 3:** Certificate/Key Exchange Test at the Services (or Application) layer.

### 2.3.2 FMPS-and-Partner (FP)

FMPS-and-Partner Testing verifies SSA’s system functionality and business logic interoperability with the Data Services Hub (DSH). Scenario-driven Test Cases will be used to verify both software and hardware interoperability. In most cases, CMS will coordinate the Test Data, Test Cases, and Test Scenarios. FMPS-and-Partner testing may also be merged with Business driven Scenarios and Test Cases.

FMPS-and-Partner Testing for Services verifies FMPS to Federal Partner Core Verification and Eligibility Interactions for FFM, SBM and Medicaid/CHIP.

It will be the responsibility of SSA to deploy the Test Data into its respective User Interface (UI)/applications and/or back-end systems.

### 2.3.3 Performance Stress Test (PST)

The Federal Hub Performance Stress Test (Fed HUB PST) verifies the responsiveness, capacity, and scalability of FFM Gateway Services and DSH Services in a one-on-one manner between CMS and SSA.

The goals of Fed HUB PST are to:

- Verify Service availability using peak loads (see Service Level Agreements)
- Measure Service response times
- Measure infrastructure utilization, capacity, and scalability
- Determine impact of outages if Services are unavailable ('down')
- Measure Error Rates, e.g., Time Outs, Invalid Responses, etc.

FFM UI PST verifies the functionality and availability of the FFM-User Interface (FFM UI) and Data Services Hub Services across a Multi-Agency environment with select Federal Partners.

The goals of FFM-UI PST are to:

- Verify Multi-Agency Integration, i.e. a simulcast between select Federal Partners (Verifications and MEC)
- Verify that the FFM-UI is capable of invoking Federal Verification and MEC Services using peak loads (see Service Level Agreements)
- Measure Web Page and Service response times
- Measure Infrastructure utilization, capacity, and scalability
- Determine impact of outages if Services are unavailable ('down')
- Measure Error Rates, e.g., Time Outs, Invalid Responses, etc.

### **2.3.4 End-to-End (E2E) / Regression Test (RT)**

End-to-End Testing verifies system functionality and interoperability across a Multi-Partner environment, i.e. with all Partners. Testing will be based upon Eligibility and Enrollment scenarios to ensure that:

- The Federally-Facilitated Marketplace (FFM) (optionally State Based Marketplaces (SBMs), Medicaid and CHIP) can consume a full range of applications and generate appropriate requests to the DSH;
- The DSH can generate requests to Partners;
- Partners can generate responses from their test databases and the FFM can generate correct outcomes.

Approximately 636 applications with identical functional data will be provided to each eligibility source (FFM, SBM, Medicaid and CHIP, and 3 Issuers). This will cover the 'Happy Path' that will match the data embedded in the Partners test environments and include additional individuals and Tax Households that will not match ('Unhappy Path').

Prior to the beginning of End-to-End testing, Regression Testing (RT) will be conducted between CMS and each participating Partner. Regression Testing selectively re-tests system functionality and interoperability after the deployment of Release 6 code, i.e. to validate that Release 6 code has not caused any unintended modifications and/or results with specific system requirements.

### **2.3.5 Production Readiness (PR)**

Production Readiness Testing verifies connectivity between the Federal Marketplace Program System (FMPS) production environment and other Partners' production environments.

## **2.4 Test Environment Profile**

SSA will use its own Testing Environment(s), and information about the locations and access requirements will be coordinated with CMS prior to Test Execution. Test Environments are expected to support all Marketplace related applications, interfaces, and data necessary for Test Execution. The following is a list of SSA environments:

- Development Environment: Used for software development and unit testing.
- Validation Environment: Used for internal SSA Validation Testing; External Testing during FMPS-and-Partner functional testing period. External access to validation environment will be restricted during Phase II of internal SSA Validation Testing.
- Integration Environment: Production-like environment for Performance Stress Testing (PST).

CMS will use its external Test environments (IMP1A and IMP1B). Pertinent information regarding CMS' Test Environment will be communicated to SSA during recurring Integrated Project Team (IPT) meetings.



### 2.4.1 Test Environment Operations and Scheduling

Detailed information regarding SSA's Test Schedule will be communicated during Integrated Project Team (IPT) meetings. Since various Partners will be sharing one test environment for the execution of Test Types, CMS will employ a "time slicing" approach by providing each Federal Partner with a three-hour time window in which to carry out relevant tests.

The following **Table** captures high-level Test Schedule details for SSA:

**Table 3: Test Environment Schedule (Current as of April 26, 2013)**

Environment / Release	Schedule		
	Agency	Key Date (s)	Time
IMP1 / Release 5	SSA	5/8 – 6/28	Various time blocks
IMP1 / Release 6	SSA	8/20 – 8/30	End-to-End Testing

### 2.4.2 Test Environment Security

Security standards and pre-requisites that are required for SSA include the following:

- Obtain, exchange, and install security certificates needed for connectivity with the web service(s)
- Exchange end-points addresses needed for connectivity with the web service(s)
- Submit request to open the port(s) on the respective firewall(s)

### 3 Testing Process

This **Section** is organized into the following Sub-Sections:

- Roles and Responsibilities (All Leads)
- Test Readiness
- Test Tools
- Test Validation
- Test Reporting

Each subject will be discussed in more detail in the following **Sub-Sections**:

#### 3.1 Roles and Responsibilities (All Leads)

The following **Table** identifies the Federal Leads and supporting Contractors from CMS and SSA:

**Table 4: Roles and Responsibilities (All Leads)**

Role(s) / Functional Area(s)		Points-of-Contact (POC)
CMS Lead(s)	Test Coordinator(s)	Richard Speights (CMS)
	Test Technical Advisor(s)	Paul Donohoe (CMS / CIISG)
	Development Technical Advisor(s)	Daniel Lazenby (CMS / CIISG)
	CMS Business Requirements	CMS Business Owners (CCIIO and CMCS)
	Formal Test Execution / Schedules	QSSI - ACA Test Team
	Test Schedules; Support; Test Harness	QSSI - Development Team
	Test Data	Mathematica
	User Interface (UI) Support	CGI - Development Team
	Error Handling/Incident Management	Walt Dill (CMS)
	Change Control (CC)	Reba Cole (CMS)
SSA Lead(s)		Mark Wicker (SSA) Patricia Berlin (SSA)

#### 3.2 Test Readiness

SSA is required to complete a number of pre-requisite artifacts prior to formal Test Execution:

- Interface Control Document (ICD) / Business Service Description (BSD)
- Test Readiness Checkpoint (TRC)
- Test Readiness Review (TRR)

##### 3.2.1 Interface Control Document (ICD) / Business Service Description (BSD)

CMS and SSA are responsible for developing an Interface Control Document (ICD) and associated Business Service Description (BSD), i.e. to capture a common set of formats, methods, and protocols required to effectively define the interface between the CMS and SSA.

SSA's ICD was base-lined on October 12, 2012.

##### 3.2.2 Test Readiness Checkpoint (TRC)

SSA is responsible for completing a *Test Readiness Checkpoint (TRC)*, i.e. to document the high-level Test Readiness between the CMS and SSA.

A template TRC is provided in **Appendix B**.

##### 3.2.3 Test Readiness Review (TRR)

SSA is responsible for completing a *Test Readiness Review (TRR)*, i.e. to document a testing "Go/No-Go" decision based on a jointly-defined checklist of required criteria.



A template TRR is provided in **Appendix B**.

### 3.3 Test Tools

SSA is encouraged to consider the following **Table** for suggested Test Tools:

**Table 5: Test Tools**

Tool	Purpose
SoapUI Pro	Data Services Hub (DSH) Testing
Collaborative Application Lifecycle Tool (CALT)	Overall tracking and requirements/Test Cases/Defects management
Quick Test Professional (QTP)	Functional automated Test script execution/regression
LoadRunner	Performance Stress Test (PST)
BrowserStack	Cross browser Testing
Excel Spreadsheet	Defect Tracking
Collaborative Application Lifecycle Tool (CALT)	Configuration Management

### 3.4 Test Validation

Test Execution is based on the following assumptions:

- A successful TRR has been completed
- Defect data will be collected on a common spreadsheet
- All new Defects discovered by Interagency Testing will be recorded on the spreadsheet
- Testers will record Test results
- Test "management" will monitor Test activities, review Defect data, and generate/approve the Defect report
- Defect "ownership" may not be immediately known
- Scheduled system and/or data refresh will occur between 6:00 p.m. and 7:00 a.m. EST
- Major issues or problems will be reported immediately; examples include:
  - Problems with testing infrastructure (passwords, scripts, tools, environments, etc.)
  - Defects that block significant numbers of downstream Tests
- An open communication line (established conference call number) will be established for each day's Testing to be used by Test leads when issues that require discussion occur

(b)(5)

### 3.5 Test Reporting

A Weekly Interagency Test Status Report will capture the progress of testing activities:

- Total number of Test Cases in the inventory
- Number of Test Cases planned to be executed
- Number of Test Cases executed
- Number of Test Cases passed
- Number of Test Cases failed
- Number of Test Cases not run, deferred, and/or waived
- Summary (and counts) of Defects reported, i.e. by Severity Levels and subtotals for each Severity Level

## 4 Additional Processes

This **Section** is organized into the following Sub-Sections:

- Error Handling Testing
- Issue / Defect Management
- Change Control (CC) Management

Each subject will be discussed in more detail in the following **Sub-Sections**:

### 4.1 Error Handling Testing

SSA's Error Code Descriptions and Data Services Hub (DSH) responses are as follows (**Current as of April 1, 2013**):

SSA Error Code Description	Hub Response Code	Hub Response Description
Authentication Failure	(b)(5)	Unexpected Exception occurred at Trusted Data Source
Internal Error (from server)	(b)(5)	Unexpected Exception occurred at Trusted Data Source
Schema validation failure	(b)(5)	Unexpected Exception occurred at Trusted Data Source
General Internal Error	(b)(5)	Unexpected Exception occurred at Trusted Data Source
Bad transaction. SSA could not complete transaction	(b)(5)	Trusted Data Source System Unavailable

### 4.2 Issue / Defect Management

The validation of FMPS-and-Partner (FP) Test Results will be the responsibility of the FMPS Independent Test Team. During the testing of SSA's interactions (as a part of FP) Test Cases are used to provide a measure of success.

A record of an Issue / Defect must be created to document any condition that occurs during testing where the expected result for a test step does not match the actual result. The record can be logged via email or phone. A severity level and priority is designated during the FMPS Defect Management Workflow. Responsibility for troubleshooting and resolution is assigned to the appropriate area of FMPS operations by the triage specialists within the Marketplace Operations Support Center (XOSC) Help Desk.

Severity levels are translated as follows to better represent the impact placed upon testing:

**Table 6: Severity Levels**

Severity	Description
S1- Critical	The Defect is a "showstopper", which means that operational functions, mission critical functions, and testing activities cannot be performed.
S2 – Severe	The Defect impacts operations and / or degrades functionality; however, a workaround is available such that testing may still be performed.
S3 – Moderate	The Defect indicates a requirement is not met; however, the Defect does not hinder mission critical functions, operations, or testing. Further, if the Defect was NOT corrected an end user could still perform the functions of the system without adverse impact.
S4 – Irritant	Results in user / operator inconvenience or annoyance, but does not affect a required operational or mission essential capability.

As part of the Defect Management workflow, all Issues / Defects are reviewed by the XOSC triage specialists to determine the appropriate course of action based on the severity and priority of the issue.

Issue / Defects that are not anticipated to be closed immediately will be scheduled to be fixed and placed into a queue for the Development Team to address. On both a scheduled and emergency basis, new application releases incorporating fixes will be verified internally and then moved into the external Test Environment. If SSA is still within its Test Execution period, it will re-test the area affected by the Issue / Defect.

#### 4.2.1 Defect Management Workflow

The FMPS Independent Test Team/Federal Agency who uncovers an Issue / Defect must communicate the nature of the Issue / Defect to the Marketplace Operations Support Center (XOSC) Help Desk. Options include:

- Email: (b)(5)@MS.HHS.Gov
- Phone: 1-855-CMS-1515

The Help Desk opens a trouble ticket, performs an initial evaluation, and sends the Issue / Defect to the appropriate FMPS operational team to further analyze and troubleshoot (DSH & FFM contractors and the FMPS Independent Testing Team).

- The recipient team is responsible for verifying the initial severity and priority ratings and determining the appropriate repair.
- Status of Defects can be verified by the submitter by contacting the XOSC or visiting the CALT interface to search the Remedy ID.
- Resolution is coordinated through Regional Technical Support (RTS) and the OIS IT Project Manager (PM) or Medicaid Enrollment and Eligibility systems analyst.

#### 4.2.2 Tracking Issues / Defects

The information pertaining to the issue will be captured in the XOSC trouble ticket system. When a tester encounters an Issue / Defect, testing should continue for the remaining steps of the Test Case (if possible), and all subsequent Issues / Defects will be logged.

As Issues / Defects are identified during testing, they are initially recorded in the XOSC trouble ticket system and then moved to the Defect management system of the FMPS Operational team that is assigned ownership. Defect management reports are built through a joint Issues / Defect tracking spreadsheet. The details of the data collected are shown in the following **Table**.

**Table 7: Issue / Defect Tracking**

Data Element	Description
Date Identified	Date of test
Test Case Identifier	Identification number from the Test Case
Test Steps Causing Defect	Step number from Test Case
Test Phase	Test Type
CMS Defect Identifier	Identifier filled in for CMS reported Defects
Federal Defect Identifier	Identifier filled in for Federal reported Defects
Status	Current Defect status (open, closed, deferred)
Escalation	The person an unresolved Defect has been sent to for resolution
CMS Version Number	Identification number for the CMS system being tested
Federal Version Number	The identification number for the Federal system being tested
Defect Title	The name of the Defect
Defect Description (Brief)/Symptoms	A description of the Defect and the symptoms exhibited
Defect Severity	The severity of the Defect; the severity level indicating the degree the Defect impedes system operations (S1 – Critical, S2 – Severe, S3 – Moderate, S4 – Irritant, S5 – Documentation/Process)
Defect Priority	The priority of the Defect; the priority level indicating the relative importance of repairing the Defect (P1 – Urgent, P2 – High, P3 – Medium, P4 – Low). A Defect with a high priority (irrespective of its severity level) will be fixed.
Defect Source	The location where the Defect was introduced into the system (not necessarily the location where the Defect exists now)
Estimated Repair Date (Version)	The date when the repair will be corrected; version containing repair
Notes	Any notes or comments for the Defect

#### 4.2.3 Testing and Retesting Issues / Defects

Issues / Defects will be evaluated by the FMPS program management team and may result in updating the application to address the issue. Upon identification of defect severity and priority, each issue / defect shall be submitted to the CR process (Section 4.3) for handling and eventual disposition. Once approved and scheduled for its respective release to the build process, each defect resolution will be migrated into the Test Environment and the Federal Agency tester will be asked to execute the steps again to verify that the issue has been successfully resolved.

The FMPS program CR management team may decide to "Defer" a Defect fix depending on the nature and severity of the Defect. In this situation, the tester may complete their assignment with Test Cases that are still in the "Failed" state. It is feasible that a tester may be contacted after the testing phase to assist with the validation of a software refinement to resolve a "Failed" Test Case.

### 4.3 Change Control (CC)

Changes to base-lined work products must be communicated by SSA to CMS via a Change Request (CR), and managed through the Interagency Change Control (CC) Management process.

Federal Agencies proposing changes to jointly-owned base-lined documents (or changes that may impact multiple/all-Agencies) are required to utilize the Interagency CR process, i.e. as part of the Interagency CC Management process. The defined CC process ensures the coordinated evaluation; tracking; analysis; review; disposition; and reporting of CRs.

If SSA has any questions regarding this CR/CC process, please contact the CMS Change Control Coordinator, Reba Cole at [Reba.Cole@cms.hhs.gov](mailto:Reba.Cole@cms.hhs.gov).

DRAFT

## 5 Test Data, Scenarios, and Cases

This **Section** is organized into the following Sub-Sections:

- Test Approach
- Test Data
- Test Scenarios and Cases
- Test Execution

Each subject will be discussed in more detail in the following **Sub-Sections**:

### 5.1 Test Approach

CMS and SSA will coordinate a number of activities to ensure a successful Interagency Testing effort. A common suite of Test Data, Scenarios and Cases will be developed jointly by CMS and the Federal Agencies.

SSA data is central for CMS's approach to testing and Test Data development. CMS is designing its Test Data for thorough End-to-End testing; as such, it will be the glue that ensures that the entire system integrates properly. Central to this design are the individuals and households composed of these individuals that will reside in each partners' backend systems. SSA is providing these individuals — their Social Security Numbers (SSNs), Dates of Birth, and Names as well as additional SSA-specific data. With these individuals, CMS will create people and households for the Partners, as well as Payloads and applications for the Test Execution contractors.

Test Data will be developed prior to the execution of Interagency Testing, and made available to SSA to Test both Agency/CMS specific Interactions and specific Test Scenarios within each type of Interaction. Because SSA is the source for all individual data, CMS does not need to provide SSA with any additional test data to SSA. Once Interagency Testing officially begins, Test Data will be sufficiently comprehensive to be used for all Test Types, e.g., FMPS-and-Partner, Performance Stress, and End-to-End Testing.

Only de-identified Test Data will be created and used for Interagency Testing.

The following **Table** includes a High level schedule of Test Data delivery dates:

**Table 8: Test Data Development/Delivery Schedule (Current as of May 2, 2013)**

Test Type	Agency	Mar	Apr	May	Jun	Jul	Aug	Sep	Tasks
FMPS-and-Partner	SSA			5/8 (Delivery to Data Services Hub (DSH))  5/22 Delivery to Test Execution Contractor					<ul style="list-style-type: none"> <li>• Provide Payloads to Data Services Hub (DSH) and Test Execution contractor</li> </ul>
Performance Stress Test (PST)	SSA			5/1 Received individuals for PST  5/8 - 5/22 Delivery of Payloads to Test Execution Contractor					<ul style="list-style-type: none"> <li>• Receive 1.5M records</li> </ul>
End-to-End	SSA			5/8 Delivery to Data Services Hub (DSH)  5/22 Delivery to Test Execution Contractor					

### 5.2 Test Data, Scenarios, and Cases

The definition, generation, storage and coordination of Test Data are an important part of the Interagency Test Approach. CMS shall provide common Test Data and Scenarios designed to Test Interactions between CMS and SSA. CMS, in coordination with other Federal Partners, is developing Test Data that will enable Federal Partners to participate in full End-to-End Testing.



## 5.2.1 Test Data Development

CMS's approach to the development of Test Data focuses on two goals:

- Design Test Data to perform End-to-End testing:  
To design the End-to-End Test Data requires that all Partners have a common set of people, i.e., the same people with the same SSNs need to be used in every application. To accomplish this goal, the Social Security Administration (SSA) will provide the seed data (individuals) that will be used to create the Tax Households (THHs) and Medicaid Households (MHHs). All Federal Agencies will import the THHs, MHHs, and individuals in their respective back-end databases so that when the Data Services Hub (DSH) calls the relevant services, the necessary information will be in the Agencies' databases.
- Provide a comprehensive set of Test Data that can be used for a wide range of Scenarios as possible:  
Providing a common Test Bed allows CMS and various external Partners to perform End-to-End testing. To ensure that the maximum number of Test Cases and Scenarios are tested, it is critical to create applications, THHs, and MHHs that cover all possible Test Scenarios.

Based on the analysis, 5,125 individuals, 915 Tax Households (THH), and 461 additional Medicaid Households (MHH), and 636 applications are needed for end-to-end testing.

**Figure 1 in Appendix D** displays the relationships among the various models. Applications are composed of THHs and MHHs. **Table 1 in Appendix D** provides the logic behind the application model. The application can have between 0 to 5 THHs and 0 to 3 additional MHHs. CMS is systematically designing applications to include all combinations of THHs and MHHs identified in **Table 1**. In addition, to test extreme values in the number of households, one application will be created with 15 THHs and 5 additional MHHs.

To develop these applications, CMS created a THH model and a MHH model.

The THH model incorporates three variables:

- **Tax Filing Status** helps identify the marital status of the tax filers as well as how many tax returns the THH contains.
- **Percent Federal Poverty Level (FPL)** impacts the THH's and the members of the THH's insurance eligibility for Federal programs such as Medicaid and CHIP, as well as subsidies, such as the advanced payment of the tax credit (APTC). There are eight (8) percentages that must be tested. In addition, boundary conditions need to be tested as well, which equals 24 discrete percent FPLs needed for full testing.
- **Number of Dependents** identifies the number of dependents on the THHs tax returns. Based upon data from the census, having up to seven (7) dependents covers approximately 95 percent of the U.S. population.

When creating the THHs, the various combinations of percent FPL are incorporated from the IRS Verification Model (**Table 2 in Appendix E**) that displays the various combinations of data elements and outcomes needed to fully test the IRS verification.

The MHH requires the incorporation of another layer of logic to the creation of Test Data. The MHH model focuses on three criteria (**Table IIC in Appendix D**):

- **The Number of Additional People** needed to fill the MHH.
- **Pregnancy** also can lead to the creation of a MHH.
- **The Exceptions** which can take one of three values: non-filer, non-custodial, and non-parent.

The THHs and MHHs constrain the types of individuals needed to populate these households. At the same time, individuals populating the applications have constraints upon them imposed by the various verifications, including Social Security Administration (SSA), Minimal Essential Coverage (MEC), and Department of Homeland Security (DHS) verifications. The SSA verification model (**Table 1 in Appendix E**) organizes this variation in 13 groups that cover all of the successful and unsuccessful paths. This verification only occurs if the individual reports and SSN. SSA verifies the SSN by comparing the SSN, the name, and the month and year of birth. If the individual's information on these three fields matches the information in SSA's database, the SSN is verified. In addition, SSA verifies whether the person is alive, a citizen, or incarcerated.

The MEC verification checks (**Table 3 in Appendix E**) to see if the individuals are eligible for the following Federal health insurance plans: TRICARE, VHA, Medicaid, CHIP, Medicare, Peace Corps, or OPM. These insurance plans can cover individuals for the entire time period for which they are applying, part of the period for which they are applying, and for no part of the time period for which they are applying.

Lastly, the DHS verification model (**Table 4 in Appendix E**) assesses whether individuals are lawfully present and eligible to apply for health insurance through a Marketplace. Determining lawful presence involves many different documents, various identifications, and can require up to three steps in the verification process.

Within these constraints, CMS has incorporated a person model that identifies the key attributes of these people. This model identifies twelve characteristics: (1) Citizenship, (2) Lawful Presence, (3) Refugee, (4) Disability, (5) Pregnant, (6) Former Foster Care, (7) Indian status, (8) Full-time Student, and (9) age, as well as (10) incarceration, (11) deceased, and (12) MEC participation. The combinations of these 12 characteristics drive the logic about the people.

In addition to the logic drivers for each of these models, the application contains many additional data elements. For example, addresses and employer names are necessary for the application process, but the actual addresses and employer names have limited impact on the Marketplaces' decision making processes. For these and other application fields that are not FFM logic drivers, data element values a random generator will select values based upon specific rules that are programmed into the generator.

Developed applications will be imported into a Test Database that is under-development. This database will contain the application data and generate the expected outcome for the applications and all DSH interactions.

### 5.2.2 Test Data Deployment

From the Test Data deployment perspective, two issues must be addressed:

- First, an indexing scheme must be created to provide the QSSI – ACA Test Team with key characteristics of the applications and Payloads. Using this indexing scheme, the QSSI – ACA Test Team will be able to find specific cases to test specific functionality of the FFM and DSH.
- Second, Test Data must be delivered to the QSSI - ACA Test Team.

Because of the changing policy landscape and the staggered development cycle of the HIM, testers need to be able to identify the characteristics of the test applications and Payloads. This understanding allows the testers to ensure that they are testing the key components available for the release and sprint being tested. To accomplish this goal, a set of application characteristics and a set of Payload characteristics were created.

The application characteristics identify 23 categories of information that testers may need in their Test Data. For example, the citizenship status characteristics are essential when testing the DHS logic. The FPL of the household is necessary when determining eligibility for a variety of insurance options. **Table 1 in Appendix F** provides a detailed list of characteristics associated with applications. Since an application can contain multiple THHs and MHHs, it is only determined if the households and people on the application have the characteristics. The number of people or which households meet the characteristics are not identified.

The Payloads are also essential elements for testing the system. Simply put, Payloads transfer information among the requesters (e.g. the SBM), the DSH, and the Trusted Data Source (TDS), e.g. SSA. There are four files, or Legs, to the Payloads. Leg 1 contains the information that the requester sends to the DSH. The DSH then transforms the data and creates Leg 2 which it sends to the TDS. The TDS verifies the information and creates a response file (Leg 3) that it sends to back to the DSH. The DSH then transforms the information from Leg 3 and sends Leg 4 to the requester.

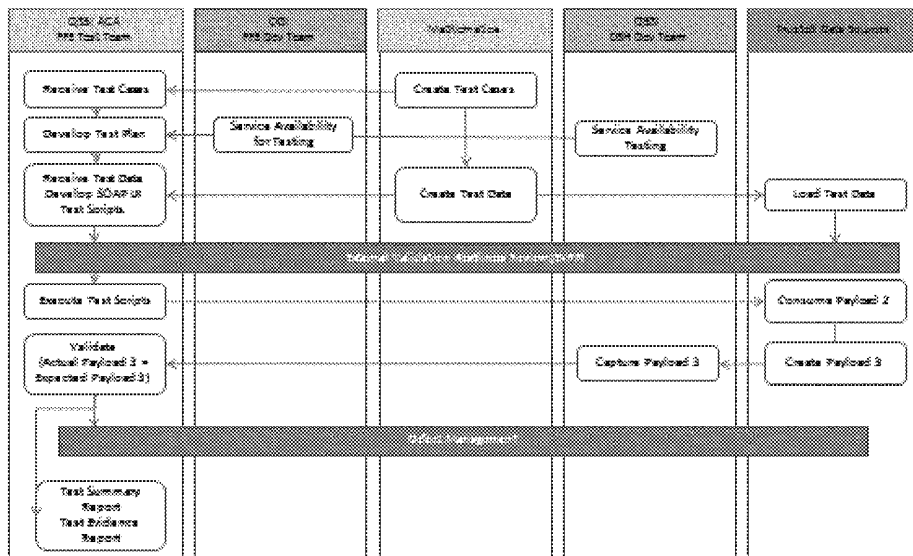
Because of the importance of the DSH and TDS, the Test Execution contractors will need to thoroughly test the system to ensure that the system accurately produces all Payloads. The Payload index in **Table 2 in Appendix F** describes the characteristics of each Payload. Specifically, it links each Payload to the master inventory ID, the TDS scenario ID, the Payload Leg, and the person ID. The characteristic index created from these IDs will help the QSSI – ACA Test Team to identify the applications, the Test Cases, and the expected outcomes used to test all interactions with the TDS.

Test Data, Test Cases and Expected Results will be provided in formats mutually agreed upon by CMS and SSA.

## 5.3 Test Execution

The QSSI - ACA Test Team will perform the necessary analysis and testing to verify that the functionality has been provided as intended. For this purpose the team will be responsible for the verification of Payload 3 as shown in the following **Figure**:

Figure 2: Test Execution Process



The QSSI - ACA Test Team will receive Test Data from Mathematica and verify Payload 3 is as expected.

- TDS will consume Payload 2 and send out Payload 3 which is captured by the QSSI – Development Team.
- QSSI - ACA Test Team will validate that Payload 3 is consumed correctly and verifies that Payload 3 matches the data provided by Mathematica.
- QSSI - ACA Test Team creates a Test Summary Report and a Test Evidence Report about the errors/Defects found during the Test Execution.

The following Services will be involved when SSA interacts with the DSH:

Table 8: Services (By Federal Agency)

Agency	Service
CMS	H10 -Appeals (Batch)
	H31 - Verify Non-Employer-Sponsored-Insurance (ESI) Minimum Essential Coverage (MEC)
	H35 -Transfer Recon File Received in XML Format (Batch)
	H38 - Monthly Medicaid/CHIP Enrollment File to CMS (Batch)
	H43 - Quarterly Eligibility Verification (Batch)
SSA	H03 - SSA Composite
IRS	H09 -Verify Annual Household Income and Family Size
	H19 - Advance Payment of the Tax Credit (APTC) Computation
	H31 - Verify Non-Employer-Sponsored-Insurance (ESI) Minimum Essential Coverage (MEC)
	H36 - Exchange Generation of Monthly and 1095 End-of-Year Reporting to IRS (Monthly)(Batch)
	H41 -Exchange Generation of Monthly and 1095 End-of-Year Reporting to IRS (Annual)(Batch)
DHS	H04 - Verify Lawful Presence (VLP) Steps 1,2,3
	H05 - VLP Send Documents (with G-845 Form). Electronically
	H07 - VLP Close Case
	H48- VLP Retrieve Resolution
VHA	H31 - Verify Non-Employer-Sponsored-Insurance (ESI) Minimum Essential Coverage (MEC)
Peace Corps	H31 -Verify Non-Employer-Sponsored-Insurance (ESI) Minimum Essential Coverage (MEC)
OPM	H31 -Verify Non-Employer-Sponsored-Insurance (ESI) Minimum Essential Coverage (MEC)
TRICARE	H31 -Verify Non-Employer-Sponsored-Insurance (ESI) Minimum Essential Coverage (MEC)



## Appendix A      Acronyms

Acronym	Definition
ACA	Affordable Care Act
BSD	Business Service Descriptions
CALT	Collaborative Application Lifecycle Management Tool
CCB	Change Control Board
CCIO	Center for Consumer Information and Insurance Oversight
CHIP	Children's Health Insurance Program
CIISG	Consumer Information and Insurance Systems Group
CM	Configuration Management
CMCS	Center For Medicaid and CHIP Services
CMS	Centers for Medicare & Medicaid Services
CR	Change Request
DHS	Department of Homeland Security
DSH	Data Service Hub
E&E	Eligibility and Enrollment
EES	Enterprise Eligibility Service
ESI	Employer-Sponsored Insurance
FMPS	Federal Marketplace Program System
FFM	Federally-Facilitated Marketplace
HHS	Health and Human Services
HIM	Health Insurance Marketplace
ICD	Interface Control Documents
IRS	Internal Revenue Service
MAGI	Modified Adjusted Gross Income
MEC	Minimum Essential Coverage
OPM	Office of Personnel Management
PR	Production Readiness
PST	Performance Stress Test
QHP	Qualified Healthcare Plan
QTP	Quick Test Professional
RTS	Regional Technical Support
SAVE	Systematic Alien Verification for Entitlements
SBM	State-Based Marketplace
SC	Secure Communication
SFTP	Secure File Transfer Protocol
SOAP	Simple Object Access Protocol
SSA	Social Security Administration
SSN	Social Security Number
TDS	Trusted Data Source
TRC	Test Readiness Checkpoint
TRR	Test Readiness Review
UI	User Interface
VHA	Veterans Health Administration
XOC	Marketplace Operations Center

## Appendix B Test Readiness Checkpoint (TRC) and Test Readiness Review (TRR)

The *Test Readiness Checkpoint (TRC)* establishes a method for documenting the test readiness of the Federal Agency along with the relevant stakeholders that will be participating in inter-agency testing.

### Test Readiness Checkpoint (TRC): Web Services Version

Item #	Title	Responsible Agency/Organization	Criteria Satisfied (Yes / No)	Comments
Obtained via FOIA by Judicial Watch, Inc.	<b>1 Documentation</b>			
	a. Have all ICDs been base-lined?			
	b. Have all BSDs been base-lined?			
	<b>2 Development</b>			
	a. Is the web service developed, tested, and ready for consumption?			
	b. If not, what is the percentage complete?			
	c. Have WSDLs been exchanged with CMS?			
	d. Have schemas been exchanged with CMS?			
	<b>3 Security</b>			
	a. Have security certificates needed for connectivity with the web service been obtained?			
	b. Have security certificates needed for connectivity with the web service been exchanged?			
	c. Have security certificates needed for connectivity with the web service been installed?			
	d. Have end-points addresses needed for connectivity with the web service been exchanged?			
	e. Have the request to open the port(s) on the respective firewall(s) been approved?			
	<b>4 Test Environment</b>			
	a. Has the Test Environment that will be used for inter-agency testing created?			
	b. Will the Test Environment be used exclusively for ACA inter-agency testing?			
	c. If no, has a schedule been established for ACA inter-agency testing?			
	d. Have all of the capabilities and dependencies for the Test Environment been implemented for inter-agency testing?			
	e. Have primary and secondary point of contacts for all support personnel been identified and contact information distributed?			

5	<b>Testing Schedule</b>			
	a. Are all parties aware of the test planning and Test Execution schedule for inter-agency testing?			
	b. Are all parties in agreement with the timelines and milestones for test planning and Test Execution?			
6	<b>Test Planning</b>			
	a. Have members of the Integrated Project Team (IPT) been identified?			
	b. Have the scope for inter-agency been defined?			
	c. Have the test scenarios that will be used for inter-agency testing been identified?			
	d. Has there been an established approach for test case development?			
	e. Have the source for test data been identified?			
7	<b>Final Disposition</b>			
	a. Have all test readiness checkpoint questions been satisfied? If no, add open items to the Action Items table.			
	b. Is a follow-up meeting to discuss the open items necessary? If yes, schedule a follow-up meeting?			

#### Test Readiness Review (TRR):

The *Test Readiness Review (TRR)* establishes a method for documenting the test readiness of each Federal Agency along with the relevant stakeholders that will be participating in Interagency Testing.

#### DRAFT – Test Readiness Review (TRR): Web Services Version

Item #	Title	Responsible Agency/Organization	Criteria Satisfied (Yes/No)	Comments
1	<b>Documentation</b>			
	a. Is the ICD for [insert TDS name] been approved by CMS and [insert TDS name]?			
	b. Is the Inter-Agency Test Plan for [insert TDS name] approved by CMS and [insert TDS name]?			
2	<b>Test Scenarios/Test Cases/Test Procedures</b>			
	a. Have the test scenarios been developed and prioritized by the business owner?			
	b. Have the test scenarios been approved by the business owner?			
	c. Have the required test cases and test procedures been completed?			
	d. Have the test cases and test procedures been placed under CM control?			
3	<b>Test Data</b>			
	a. Have the test data that will be used to support inter-agency testing been created and verified?			
	b. Have the test data been loaded to the appropriate databases or test harness?			
	c. Have the test data been placed under CM control?			
4	<b>Test Schedule</b>			
	a. Have the test schedule that will be used to support inter-agency testing be defined and agreed upon by all of the relevant stakeholders?			
	b. Does the test schedule reflect the agreed upon testing priorities and available resources?			
	c. Has a method for status reporting and frequency been established and agreed upon?			
5	<b>Defect Management</b>			
	a. Have all relevant stakeholders agreed upon a defect tracking process that will be used for inter-agency testing?			
	b. Have all testers and developers have access to the defect tracking tool?			
	c. Has an escalation process been defined for defect resolution?			
	<b>Test Environment</b>			

Item #	Title	Responsible Agency/Organization	Criteria Satisfied (Yes/No)	Comments
	a. Have network connectivity between the hub and the [insert TDS name] been established?			
	b. Have limitations and constraints to the Test Environment been disclosed to all of the relevant stakeholders?			
	c. Is the Test Environment properly configured, operational, and ready to start Test Execution?			
7	<b>Secure Communications</b>			
	a. Have all security prerequisites for secure communication between the hub and the TDS been satisfied?			
	b. Have application connectivity between the hub and the TDS been established?			
	c. Have all secure communication test cases been successfully verified?			
8	<b>Limitations &amp; Constraints</b>			
	a. Does the product documentation describe all known issues or broken functionality in the system as delivered per the Release Plan?			
	b. Are there outstanding problems from previous test phases?			
	c. Are there tests that cannot be fully or partially executed?			
9	<b>Integrated Project Team Support</b>			
	a. Has the contact list been developed and distributed to all relevant stakeholders?			
	b. Have test support requirements, hours, and procedures been agreed to by the relevant stakeholders?			
	c. Have all testers been identified and confirmed?			
10	<b>Final Disposition</b>			
	a. Have all entrance criteria been met? If no, which criteria were not demonstrated ( <i>enter in comments column</i> )?			
	b. Is a follow-up TRR needed? If yes, provide new date in the comments column.			

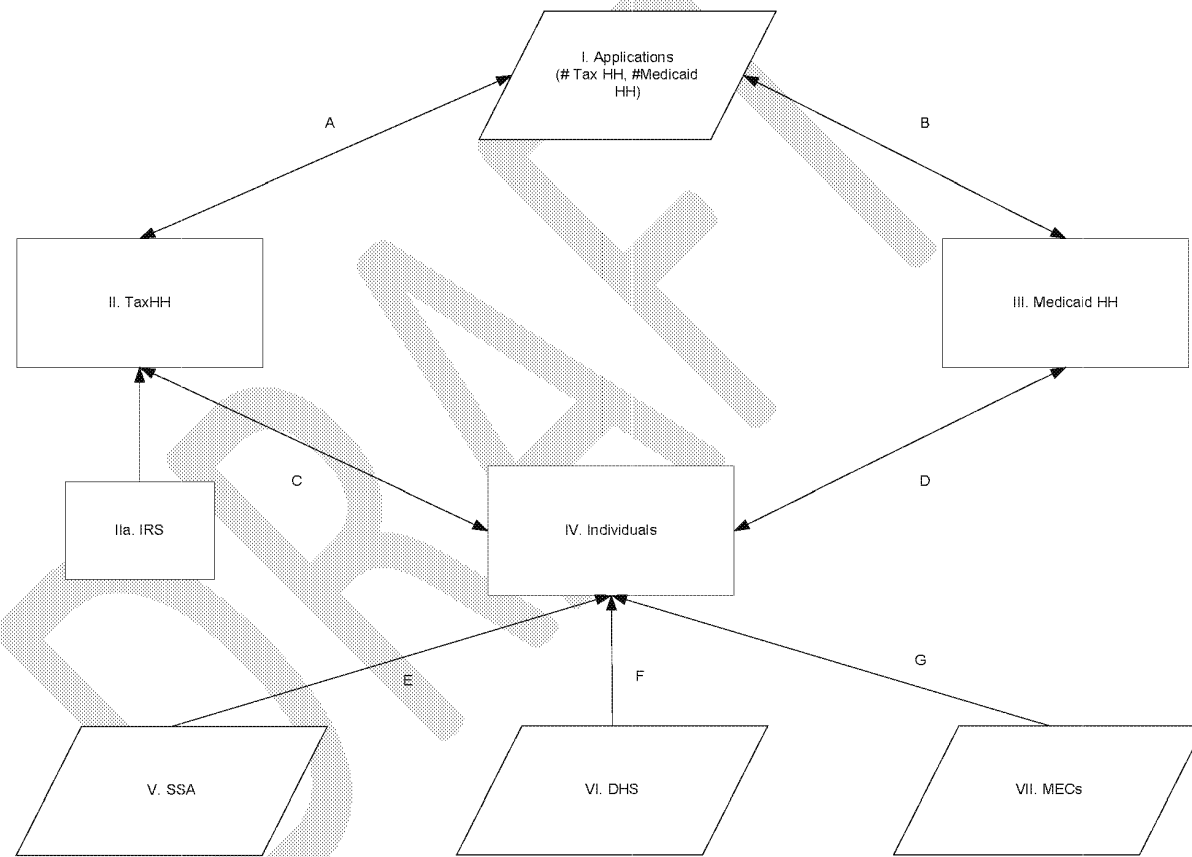
## Appendix C      Attachment 1: Theoretical Required Root Test Cases

### Summary of the Theoretical Required Root Test Cases

A. #	B. Category	C. Federal Partners SSA-IRS-DHS	D. No. of Root Test Individuals	E. Tax Households	F. Medicaid Households	G. Comments
1			104			Will use all 104 step 1 lawful presence verification cases that contain SSNs are for SSA-IRS-DHS records.
2						Based on our household model, the average household has 4 people. Thus, we need 3,072 individuals. Subtracting the 77 of SSA-IRS-DHS individuals from the 3,072 individuals provides us with 2,995 SSA-IRS data.
	Federal Partners	SSA-IRS	2,995	768	864	The 864 Medicaid Households comes 768 Tax Households that are also Medicaid Households plus an additional 96 Medicaid Households derived from the four categories of Medicaid Households (non-parent, non-custodial, married filing separately, and non-filers) as well as the 24 % FPL categories.
3		IRS-DHS	0			IRS-DHS cases are very rare. Furthermore, according to QSSI and CGI staff who gathered the requirements, IRS verification for any non-citizens who do not have an SSN is a manual process, which is outside the scope of our Test Data.
4		SSA-DHS	0		N/A	The SSA-IRS-DHS would be used to test the SSA-DHS conditions.
5		SSA Only	3	N/A		There are only 3 SSA scenarios that are SSA only—if the person is dead, a citizen who is an inmate, and a non-citizen who is an inmate.
6		DHS Only	40			Test a small number of cases that do not have an SSN.
7		IRS Only	0			There are no situations where a person can receive IRS verification without first going SSA first.
8	Insurance Providers	MEC	392	N/A	N/A	The MEC test cases require a combination of partners and start and end dates leads us to 392 cases. All of these cases could be covered in the 3,072 needed above.
10		SSA	3,075	N/A	N/A	Summing the results by partner.
11	Sub-Totals	IRS	3,072	768	864	
12		DHS	117	N/A	N/A	
13	Total		3,075	768	864	

## Appendix D Attachment 2 – Application Creation Process

Figure 1: Application Creation Process



## I. Application Model

	A. # of Tax HH	B. # of Additional Medicaid HH	C. Explanation
1	0-5	0-3	Applications contain combinations of tax HHs and Medicaid HHs. Every tax HH contains at least 1 Medicaid HH.
2	15	5	Include one application using extreme values.

## II. Calculating Tax and Medicaid Households

### A. Tax Household Model

A. Group #	B. # of Tax HHs	C. % FPL	D. Tax Filing Status	E. # of Dependents
1	1	Key FPLs and Associated Boundaries	Married Filing Jointly, Individual	0-7
2	2	Key FPLs and Associated Boundaries	Married Filing Separately	0-7
3	2	Key FPLs and Associated Boundaries	Married Filing Jointly, Individual	0-7
4	3	Key FPLs and Associated Boundaries	Married Filing Jointly, Married Filing Separately, Individual	0-3
5	4	Key FPLs and Associated Boundaries	Married Filing Jointly, Married Filing Separately, Individual	0-3
6	5	Key FPLs and Associated Boundaries	Married Filing Jointly, Married Filing Separately, Individual	0-3
7	15	[various]	[various]	[various]

### B. Medicaid Household Model

A. Group	B. # of People	C. Pregnant	D. Exceptions
1	0-3	Yes	Non-Filer
2		Yes	Non-Parent
3		Yes	Non-Custodial
4		No	Non-Filer
5		No	Non-Parent



C. Person Model

A.SSA/DHS Group #	B. Person Model Group #	C. SSA Citizen	D. SSA Verification Scenario(s)	E. DHS VLP	F. VLP Verification Scenario(s)	G. Refugee, not VLP	H. Disability	I. Pregnant	J. FFC	K. Indian	L. Full-time Student	M. # Possible Age Groups	N. MEC Rules
1	1	N	5	N	7 or 6-7	N	N	N	N	N	N	10	No MEC because non-citizen and not lawfully present.
2	2	N/A	N/A	N	7 or 6-7	N	N	N	N	N	N	10	No MEC because non-citizen and not lawfully present.
3	3	N	5	N	7 or 6-7	Y	N	N	N	N	N	10	No MEC because a qualified refugee would not have enough time to enroll in a MEC before becoming lawfully present and before becoming eligible for the Refugee Emergency Medicaid group.
4	4	N/A	N/A	N	7 or 6-7	Y	N	N	N	N	N	10	No MEC because a qualified refugee would not have enough time to enroll in a MEC before becoming lawfully present and before becoming eligible for the Refugee Emergency Medicaid group.
5	5	Y	1, or 2-1, 3-1, 4-1	N/A	N/A	N	N	N	N	N	N	10	Based on back-end MEC data for VHA, Medicare, and Peace Corps. Sprinkled in TRICARE, OPM, Medicaid, and CHIP manually. Only chose model groups without a MEC.
	6	Y	1, or 2-1, 3-1, 4-1	N/A	N/A	N	N	N	N	N	Y	4	
	7	Y	1, or 2-1, 3-1, 4-1	N/A	N/A	N	N	N	N	Y	N	10	
	8	Y	1, or 2-1, 3-1, 4-1	N/A	N/A	N	N	N	N	Y	Y	4	
	9	Y	1, or 2-1, 3-1, 4-1	N/A	N/A	N	N	N	Y	N	N	5	
	10	Y	1, or 2-1, 3-1, 4-1	N/A	N/A	N	N	N	Y	N	Y	4	
	11	Y	1, or 2-1, 3-1, 4-1	N/A	N/A	N	N	N	Y	Y	N	5	
	12	Y	1, or 2-1, 3-1, 4-1	N/A	N/A	N	N	N	Y	Y	Y	4	
	13	Y	1, or 2-1, 3-1, 4-1	N/A	N/A	N	N	Y	N	N	N	7	
	14	Y	1, or 2-1, 3-1, 4-1	N/A	N/A	N	N	Y	N	N	Y	4	
	15	Y	1, or 2-1, 3-1, 4-1	N/A	N/A	N	N	Y	N	Y	N	7	
	16	Y	1, or 2-1, 3-1, 4-1	N/A	N/A	N	N	Y	N	Y	Y	4	
	17	Y	1, or 2-1, 3-1, 4-1	N/A	N/A	N	N	Y	Y	N	N	5	
	18	Y	1, or 2-1, 3-1, 4-1	N/A	N/A	N	N	Y	Y	N	Y	4	
	19	Y	1, or 2-1, 3-1, 4-1	N/A	N/A	N	N	Y	Y	Y	N	5	
	20	Y	1, or 2-1, 3-1, 4-1	N/A	N/A	N	N	Y	Y	Y	Y	4	
	21	Y	1, or 2-1, 3-1, 4-1	N/A	N/A	N	Y	N	N	N	N	10	
	22	Y	1, or 2-1, 3-1, 4-1	N/A	N/A	N	Y	N	N	N	Y	4	
	23	Y	1, or 2-1, 3-1, 4-1	N/A	N/A	N	Y	N	N	Y	N	10	
	24	Y	1, or 2-1, 3-1, 4-1	N/A	N/A	N	Y	N	N	Y	Y	4	
	25	Y	1, or 2-1, 3-1, 4-1	N/A	N/A	N	Y	N	Y	N	N	5	
	26	Y	1, or 2-1, 3-1, 4-1	N/A	N/A	N	Y	N	Y	N	Y	4	
	27	Y	1, or 2-1, 3-1, 4-1	N/A	N/A	N	Y	N	Y	Y	N	5	
	28	Y	1, or 2-1, 3-1, 4-1	N/A	N/A	N	Y	N	Y	Y	Y	4	
	29	Y	1, or 2-1, 3-1, 4-1	N/A	N/A	N	Y	Y	N	N	N	7	
	30	Y	1, or 2-1, 3-1, 4-1	N/A	N/A	N	Y	Y	N	N	Y	4	
	31	Y	1, or 2-1, 3-1, 4-1	N/A	N/A	N	Y	Y	N	Y	N	7	
	32	Y	1, or 2-1, 3-1, 4-1	N/A	N/A	N	Y	Y	N	Y	Y	4	
	33	Y	1, or 2-1, 3-1, 4-1	N/A	N/A	N	Y	Y	Y	N	N	5	
	34	Y	1, or 2-1, 3-1, 4-1	N/A	N/A	N	Y	Y	Y	N	Y	4	
	35	Y	1, or 2-1, 3-1, 4-1	N/A	N/A	N	Y	Y	Y	Y	N	5	
	36	Y	1, or 2-1, 3-1, 4-1	N/A	N/A	N	Y	Y	Y	Y	Y	4	
6	37	N	5	Y	1 thru 5, or 6-1 thru 6-5	N	N	N	N	N	N	10	Not present in back-end MEC data for VHA, Medicare, and Peace Corps. We sprinkled (2.5%) in TRICARE, OPM, Medicaid, and CHIP randomly in a systematic/excel process. Only chose MECs that do not have back-end data at this time.
	38	N	5	Y	1 thru 5, or 6-1 thru 6-5	N	N	N	N	N	Y	4	
	39	N	5	Y	1 thru 5, or 6-1 thru 6-5	N	N	N	N	Y	N	10	
	40	N	5	Y	1 thru 5, or 6-1 thru 6-5	N	N	N	N	Y	Y	4	
	41	N	5	Y	1 thru 5, or 6-1 thru 6-5	N	N	N	Y	N	N	5	
	42	N	5	Y	1 thru 5, or 6-1 thru 6-5	N	N	N	Y	N	Y	4	
	43	N	5	Y	1 thru 5, or 6-1 thru 6-5	N	N	N	Y	Y	N	5	
	44	N	5	Y	1 thru 5, or 6-1 thru 6-5	N	N	N	Y	Y	Y	4	
	45	N	5	Y	1 thru 5, or 6-1 thru 6-5	N	N	Y	N	N	N	7	
	46	N	5	Y	1 thru 5, or 6-1 thru 6-5	N	N	Y	N	N	Y	4	
	47	N	5	Y	1 thru 5, or 6-1 thru 6-5	N	N	Y	N	Y	N	7	



A.SSA/DH S Group #	B. Person Model Group #	C. SSA Citizen	D. SSA Verification Scenario(s)	E. DHS VLP	F. VLP Verification Scenario(s)	G. Refugee, not VLP	H. Disability	I. Pregnant	J. FFC	K. Indian	L. Full-time Student	M. # Possible Age Groups	N. MEC Rules
	48	N	5	Y	1 thru 5, or 6-1 thru 6-5	N	N	Y	N	Y	Y	4	
	49	N	5	Y	1 thru 5, or 6-1 thru 6-5	N	N	Y	Y	N	N	5	
	50	N	5	Y	1 thru 5, or 6-1 thru 6-5	N	N	Y	Y	N	Y	4	
	51	N	5	Y	1 thru 5, or 6-1 thru 6-5	N	N	Y	Y	Y	N	5	
	52	N	5	Y	1 thru 5, or 6-1 thru 6-5	N	N	Y	Y	Y	Y	4	
	53	N	5	Y	1 thru 5, or 6-1 thru 6-5	N	Y	N	N	N	N	10	
	54	N	5	Y	1 thru 5, or 6-1 thru 6-5	N	Y	N	N	N	Y	4	
	55	N	5	Y	1 thru 5, or 6-1 thru 6-5	N	Y	N	N	Y	N	10	
	56	N	5	Y	1 thru 5, or 6-1 thru 6-5	N	Y	N	N	Y	Y	4	
	57	N	5	Y	1 thru 5, or 6-1 thru 6-5	N	Y	N	Y	N	N	5	
	58	N	5	Y	1 thru 5, or 6-1 thru 6-5	N	Y	N	Y	N	Y	4	
	59	N	5	Y	1 thru 5, or 6-1 thru 6-5	N	Y	N	Y	Y	N	5	
	60	N	5	Y	1 thru 5, or 6-1 thru 6-5	N	Y	N	Y	Y	Y	4	
	61	N	5	Y	1 thru 5, or 6-1 thru 6-5	N	Y	Y	N	N	N	7	
	62	N	5	Y	1 thru 5, or 6-1 thru 6-5	N	Y	Y	N	N	Y	4	
	63	N	5	Y	1 thru 5, or 6-1 thru 6-5	N	Y	Y	N	Y	N	7	
	64	N	5	Y	1 thru 5, or 6-1 thru 6-5	N	Y	Y	N	Y	Y	4	
	65	N	5	Y	1 thru 5, or 6-1 thru 6-5	N	Y	Y	Y	N	N	5	
	66	N	5	Y	1 thru 5, or 6-1 thru 6-5	N	Y	Y	Y	N	Y	4	
	67	N	5	Y	1 thru 5, or 6-1 thru 6-5	N	Y	Y	Y	Y	N	5	
	68	N	5	Y	1 thru 5, or 6-1 thru 6-5	N	Y	Y	Y	Y	Y	4	
7	69	N/A	N/A	Y	1 thru 5, or 6-1 thru 6-5	N	N	N	N	N	N	10	Not able to use the MEC verification services due to the fact that there is no SSN for this SSA/DHS group.
	70	N/A	N/A	Y	1 thru 5, or 6-1 thru 6-5	N	N	N	N	N	Y	4	
	71	N/A	N/A	Y	1 thru 5, or 6-1 thru 6-5	N	N	N	N	Y	N	10	
	72	N/A	N/A	Y	1 thru 5, or 6-1 thru 6-5	N	N	N	N	Y	Y	4	
	73	N/A	N/A	Y	1 thru 5, or 6-1 thru 6-5	N	N	N	Y	N	N	5	
	74	N/A	N/A	Y	1 thru 5, or 6-1 thru 6-5	N	N	N	Y	N	Y	4	
	75	N/A	N/A	Y	1 thru 5, or 6-1 thru 6-5	N	N	N	Y	Y	N	5	
	76	N/A	N/A	Y	1 thru 5, or 6-1 thru 6-5	N	N	N	Y	Y	Y	4	
	77	N/A	N/A	Y	1 thru 5, or 6-1 thru 6-5	N	N	Y	N	N	N	7	
	78	N/A	N/A	Y	1 thru 5, or 6-1 thru 6-5	N	N	Y	N	N	Y	4	
	79	N/A	N/A	Y	1 thru 5, or 6-1 thru 6-5	N	N	Y	N	Y	N	7	
	80	N/A	N/A	Y	1 thru 5, or 6-1 thru 6-5	N	N	Y	N	Y	Y	4	
	81	N/A	N/A	Y	1 thru 5, or 6-1 thru 6-5	N	N	Y	Y	N	N	5	
	82	N/A	N/A	Y	1 thru 5, or 6-1 thru 6-5	N	N	Y	Y	N	Y	4	
	83	N/A	N/A	Y	1 thru 5, or 6-1 thru 6-5	N	N	Y	Y	Y	N	5	
	84	N/A	N/A	Y	1 thru 5, or 6-1 thru 6-5	N	N	Y	Y	Y	Y	4	
	85	N/A	N/A	Y	1 thru 5, or 6-1 thru 6-5	N	Y	N	N	N	N	10	
	86	N/A	N/A	Y	1 thru 5, or 6-1 thru 6-5	N	Y	N	N	N	Y	4	
	87	N/A	N/A	Y	1 thru 5, or 6-1 thru 6-5	N	Y	N	N	Y	N	10	
	88	N/A	N/A	Y	1 thru 5, or 6-1 thru 6-5	N	Y	N	N	Y	Y	4	
	89	N/A	N/A	Y	1 thru 5, or 6-1 thru 6-5	N	Y	N	Y	N	N	5	
	90	N/A	N/A	Y	1 thru 5, or 6-1 thru 6-5	N	Y	N	Y	N	Y	4	
	91	N/A	N/A	Y	1 thru 5, or 6-1 thru 6-5	N	Y	N	Y	Y	N	5	
	92	N/A	N/A	Y	1 thru 5, or 6-1 thru 6-5	N	Y	N	Y	Y	Y	4	
	93	N/A	N/A	Y	1 thru 5, or 6-1 thru 6-5	N	Y	Y	N	N	N	7	
	94	N/A	N/A	Y	1 thru 5, or 6-1 thru 6-5	N	Y	Y	N	N	Y	4	
	95	N/A	N/A	Y	1 thru 5, or 6-1 thru 6-5	N	Y	Y	N	Y	N	7	
	96	N/A	N/A	Y	1 thru 5, or 6-1 thru 6-5	N	Y	Y	N	Y	Y	4	

A. SSN/DH S Group #	B. Person Model Group #	C. SSA Citizen	D. SSA Verification Scenario(s)	E. DHS VLP	F. VLP Verification Scenario(s)	G. Refugee, not VLP	H. Disability	I. Pregnant	J. FFC	K. Indian	L. Full-time Student	M. # Possible Age Groups	N. MEC Roles
	97	N/A	N/A	Y	1 thru 5, or 6-1 thru 6-5	N	Y	Y	Y	N	N	5	
	98	N/A	N/A	Y	1 thru 5, or 6-1 thru 6-5	N	Y	Y	Y	N	Y	4	
	99	N/A	N/A	Y	1 thru 5, or 6-1 thru 6-5	N	Y	Y	Y	Y	N	5	
	100	N/A	N/A	Y	1 thru 5, or 6-1 thru 6-5	N	Y	Y	Y	Y	Y	4	
Total person types:												556	

## Appendix E Attachment 3: TDS Verification Models

### 1. Test Scenarios for SSA Verification

A. Group #	B. Number	C. SSN Verification			D. Death	E. Citizenship Verification	F. Incarceration Verification	G. Inmate Status	H. Quarters of Coverage	I. Outcome	J. Scenario Text
		1. SSN	2. Name	3. DOB							
SSA.1		Yes	Yes	Yes	Yes	N/A	N/A	N/A	N/A	Exit Marketplace.	Individual has been verified as dead. Individual cannot enter the Marketplace.
SSA.2		Yes	Yes	Yes	No	Yes	Yes	Yes	N/A	Exit Marketplace.	Individual has been verified as currently incarcerated. Individual cannot enter the Marketplace.
SSA.3		Yes	Yes	Yes	No	Yes	Yes	No	N/A	Go to IRS Model.	Individual has been verified as a citizen, not currently incarcerated, and not dead. Individual can enter the Marketplace.
SSA.4		Yes	Yes	Yes	No	Yes	No	N/A	N/A	Go to IRS Model.	Individual has been verified as a citizen, not currently incarcerated, and not dead. Individual can enter the Marketplace.
SSA.5		Yes	Yes	Yes	No	No	Yes	Yes	N/A	Exit Marketplace.	Individual has been verified as currently incarcerated. Individual cannot enter the Marketplace.
SSA.6		Yes	Yes	Yes	No	No	Yes	No	N/A	Go to IRS Model.	Individual has been verified as a citizen, not currently incarcerated, and not dead. Individual can enter the Marketplace.
SSA.7		Yes	Yes	Yes	No	No	No	N/A	< 40 Quarters	Go to DHS-Non-Citizen Model	Individual's citizenship could not be verified, requiring quarters of coverage information. Additional lawful presence verification is needed.
SSA.8		Yes	Yes	Yes	No	No	No	N/A	40 Quarters	Go to DHS-Non-Citizen Model	Individual's citizenship could not be verified requiring quarters of coverage information. Additional lawful presence verification is needed.
SSA.9		Yes	Yes	Yes	No	No	No	N/A	> 40 Quarters	Go to DHS-Non-Citizen Model	Individual's citizenship could not be verified requiring quarters of coverage information... Additional lawful presence verification is needed.
SSA.10		Yes	Yes	No	N/A	N/A	N/A	N/A	N/A	Inconsistency Period Triggered.	Individual's Date of Birth does not match SSA's record of SSN and Name. Additional information is needed.
SSA.11		Yes	No	No	N/A	N/A	N/A	N/A	N/A	Inconsistency Period Triggered.	Individual's Name and Date of Birth do not match SSA's record of SSN. Additional information is needed.
SSA.12		Yes	No	Yes	N/A	N/A	N/A	N/A	N/A	Inconsistency Period Triggered.	Individual's name does not match SSA's record of SSN and Date of Birth. Additional information is needed.
SSA.13		No	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Go to DHS-Non-Citizen Model	SSN could not be verified. Additional lawful presence verification is needed.

### 2. Test Scenarios for IRS Verification (IRS Model)

A. Group	B. Count	C. SSN in request?	D. Tax Return Found for SSN?	E. Does name match with tax return?	F. Deceased?	G. Is individual or spouse a victim of identity theft?	H. Spouse TIN match TIN in IRS file?	I. Valid tax return found?	J. More than 1 tax return?	K. Dependent has a filing requirement?	L. Reconciled APTC in referenced tax year?	M. Outcome	N. Scenario Text
IRS.1		No	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	No SSN in request.	IRS Response Code = 004. SSN is not used in IRS Income and Family Size Verification Request.
IRS.2		Yes	No	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Tax return is not found.	IRS Response Code = 006. Tax return information is not found.
IRS.3		Yes	Yes	No	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Tax record shows SSN and name do not match.	IRS Response Code = 004. Tax return does not have the same name on file as the request.
IRS.4		Yes	Yes	Yes	Yes	N/A	N/A	N/A	N/A	N/A	N/A	Individual is dead.	IRS Response Code = 002. IRS records show that individual is currently dead.
IRS.5		Yes	Yes	Yes	No	Yes	N/A	N/A	N/A	N/A	N/A	Victim of identity theft.	IRS Response Code = 002. IRS records show that individual or individual's spouse is/are victim(s) of identity theft.
IRS.6		Yes	Yes	Yes	No	No	No	N/A	N/A	N/A	N/A	Spouse TIN does not match.	IRS Response Code = 003. IRS records show that the TIN of the spouse does not match the TIN of the spouse that is found in the tax records.
IRS.7		Yes	Yes	Yes	No	No	No	No	N/A	N/A	N/A	A valid tax return was not found.	IRS Response Code = 004. The return on file was a Form 1040PR, 1040SS, 1040C, and 1040NR which does not allow for the service to provide an accurate response.
IRS.8		Yes	Yes	Yes	No	No	No	Yes	Yes	N/A	N/A	More than one tax return on file for the same tax year.	IRS Response Code = 004. More than one tax return was found for the same file year.
IRS.9		Yes	Yes	Yes	No	No	No	Yes	No	No	N/A	No dependent filing requirement.	IRS Response Code = 008. Dependent has no filing requirement for the reference tax year.
IRS.10		Yes	Yes	Yes	No	No	No	Yes	No	No	N/A	No dependent filing requirement.	IRS Response Code = 008. Dependent has no filing requirement for the reference tax year.
IRS.11		Yes	Yes	Yes	No	No	No	Yes	No	No	No	Individual did not reconcile APTC for referenced tax year.	IRS Response Code = 007. IRS records indicate that the APTC made on the filer's behalf in the referenced tax year and the individual did not file a return reconciling the APTC available.

A. Group	B. Count	C. SSN in request?	D. Tax Return Found for SSN?	E. Does name match with tax return?	F. Deceased?	G. Is individual or spouse a victim of identity theft?	H. Spouse TIN match TIN in IRS file?	I. Valid tax return found?	J. More than 1 tax return?	K. Dependent has a filing requirement?	L. Reconciled APTC in referenced tax year?	M. Outcome	N. Scenario Text
IRS.12		Yes	Yes	Yes	No	No	No	Yes	No	No	Yes	Valid IRS Response will be returned.	IRS verification for income and family size was successfully completed.

### 3. Minimal Essential Coverage (ESI and Non-ESI) Test Scenarios

A. Group #	B. Count	C. TRICARE	D. VA	E. Medicaid	F. CHIP	G. Medicare	H. Peace Corps	I. OPM	J. Does MEC Coverage Date cover the requested eligibility dates?	K. Outcome	L. Scenario Text
MEC.1		Yes	No	No	No	No	No	No	Full	Insured fully for the coverage dates	Individual is covered by TRICARE fully for the coverage dates. Not Eligible for Medicaid, CHIP, APTC, or CSR.
MEC.2		Yes	No	No	No	No	No	No	Partial	Insured partially for the coverage dates	Individual is covered by TRICARE partially for the coverage dates. May be eligible for Medicaid, CHIP, APTC, or CSRs for the dates where there is no MEC coverage.
MEC.3		No	Yes	No	No	No	No	No	Full	Insured fully for the coverage dates	Individual is covered by VA fully for the coverage dates. Not Eligible for Medicaid, CHIP, APTC, or CSR.
MEC.4		No	Yes	No	No	No	No	No	Partial	Insured partially for the coverage dates	Individual is covered by VA partially for the coverage dates. May be eligible for Medicaid, CHIP, APTC, or CSRs for the dates where there is no MEC coverage.
MEC.5		No	No	Yes	No	No	No	No	Full	Insured fully for the coverage dates	Individual is covered by Medicaid fully for the coverage dates. Not Eligible for Medicaid, CHIP, APTC, or CSR.
MEC.6		No	No	Yes	No	No	No	No	Partial	Insured partially for the coverage dates	Individual is covered by Medicaid partially for the coverage dates. May be eligible for Medicaid, CHIP, APTC, or CSRs for the dates where there is no MEC coverage.
MEC.7		No	No	No	Yes	No	No	No	Full	Insured fully for the coverage dates	Individual is covered by CHIP fully for the coverage dates. Not Eligible for Medicaid, CHIP, APTC, or CSR.
MEC.8		No	No	No	Yes	No	No	No	Partial	Insured partially for the coverage dates	Individual is covered by CHIP partially for the coverage dates. May be eligible for Medicaid, CHIP, APTC, or CSRs for the dates where there is no MEC coverage.
MEC.9		No	No	No	No	Yes	No	No	Full	Insured fully for the coverage dates	Individual is covered by Medicare fully for the coverage dates. Not Eligible for Medicaid, CHIP, APTC, or CSR.
MEC.10		No	No	No	No	Yes	No	No	Partial	Insured partially for the coverage dates	Individual is covered by Medicare partially for the coverage dates. May be eligible for Medicaid, CHIP, APTC, or CSRs for the dates where there is no MEC coverage.
MEC.11		No	No	No	No	No	Yes	No	Full	Insured fully for the coverage dates	Individual is covered by Peace Corps fully for the coverage dates. Not Eligible for Medicaid, CHIP, APTC, or CSR.
MEC.12		No	No	No	No	No	Yes	No	Partial	Insured partially for the coverage dates	Individual is covered by Peace Corps partially for the coverage dates. May be eligible for Medicaid, CHIP, APTC, or CSRs for the dates where there is no MEC coverage.
MEC.13		No	No	No	No	No	No	Yes	Full	Insured fully for the coverage dates	Individual is covered by OPM fully for the coverage dates. Not Eligible for Medicaid, CHIP, APTC, or CSR.
MEC.14		No	No	No	No	No	No	Yes	Partial	Insured partially for the coverage dates	Individual is covered by OPM partially for the coverage dates. May be eligible for Medicaid, CHIP, APTC, or CSRs for the dates where there is no MEC coverage.
MEC.15		No	No	No	No	No	No	No	N/A	Not Insured	Individual is not eligible for other insurance. Individual may potentially be eligible for Medicaid, CHIP, APTC, or CSR.

### 4. Test Scenarios for DHS SAVE Service

A. Group #	B. Count	C. Eligible Documentation	D. Valid Request	E. SEVIS ID Required	F. Refer to Student/Visitor to Sponsor	G. Verification Match? (Step 1)	H. Verification Match (Step 2)	I. Verification Match (Step 3)	J. Five Year Bar?	K. Qualified Non-Citizen?	L. Outcome	M. Scenario Text
DHS.1		No	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Unable to invoke the SAVE service.	The presented documentation is not a document that is accepted by DHS to verify Legal presence.
DHS.2		Yes	Yes	Yes (Eligibility Code = 32)	Yes (Eligibility Code = 119)	N/A	N/A	N/A	N/A	N/A	Enter 90 day reconciliation period.	The individual must resubmit with a SEVIS ID. Individual is referred to sponsor. Individual enters into a 90 day reconciliation period.
DHS.3		Yes	Yes	Yes (Eligibility Code = 32)	No	Yes	N/A	N/A	N/A	N/A	Individual is verified as Legally present in Step 1.	The individual must resubmit with a SEVIS ID. Individual is verified as Legally present in Step 1 of the DHS service.
DHS.4		Yes	Yes	Yes (Eligibility Code = 32)	No	No	Yes	N/A	N/A	N/A	Individual is verified as Legally present in Step 2.	The individual must resubmit with a SEVIS ID. Individual is verified as Legally present in Step 2 of the DHS service.
DHS.5		Yes	Yes	Yes (Eligibility Code = 32)	No	No	No	Yes	Yes	Yes	Individual is a qualified non-citizen and cannot receive services for 5 years.	The individual must resubmit with a SEVIS ID. Individual is verified as Legally present in Step 3 of the DHS service. Individual is barred from receiving services for 5 years. The individual is a qualified non-citizen.

A. Group #	B. Count	C. Eligible Documentation	D. Valid Request	E. SEVIS ID Required	F. Refer to Student/Visitor to Sponsor	G. Verification Match? (Step 1)	H. Verification Match (Step 2)	I. Verification Match (Step 3)	J. Five Year Bar?	K. Qualified Non-Citizen?	L. Outcome	M. Scenario Text
DHS.6		Yes	Yes	Yes (Eligibility Code = 32)	No	No	No	Yes	Yes	No	Individual is not a qualified non-citizen and cannot receive services for 5 years.	The individual must resubmit with a SEVIS ID. Individual is verified as Legally present in Step 3 of the DHS service. Individual is barred from receiving services for 5 years. The individual is not a qualified non-citizen.
DHS.7		Yes	Yes	Yes (Eligibility Code = 32)	No	No	No	Yes	No	Yes	Individual is a qualified non-citizen.	The individual must resubmit with a SEVIS ID. Individual is verified as Legally present in Step 3 of the DHS service. Individual is not barred for receiving services for 5 years and is a qualified non-citizen.
DHS.8		Yes	Yes	Yes (Eligibility Code = 32)	No	No	No	Yes	No	No	Individual is not a qualified non-citizen.	The individual must resubmit with a SEVIS ID. Individual is verified as Legally present in Step 3 of the DHS service. Individual is not barred for receiving services for 5 years and is not a qualified non-citizen.
DHS.9		Yes	Yes	Yes (Eligibility Code = 32)	No	No	No	Yes	Met	Yes	Individual has met the five year bar on services and is a qualified non-citizen.	The individual must resubmit with a SEVIS ID. Individual is verified as Legally present in Step 3 of the DHS service. Individual has met the 5 year bar and is a qualified non-citizen.
DHS.10		Yes	Yes	Yes (Eligibility Code = 32)	No	No	No	Yes	Met	No	Individual has met the five year bar on services and is not a qualified non-citizen.	The individual must resubmit with a SEVIS ID. Individual is verified as Legally present in Step 3 of the DHS service. Individual has met the 5 year bar and is not a qualified non-citizen.
DHS.11		Yes	Yes	Yes (Eligibility Code = 32)	No	No	No	No	N/A	N/A	Individual is verified as not Legally present.	The individual must resubmit with a SEVIS ID. Individual is verified as not Legally present after all 3 steps.
DHS.12		Yes	Yes	No	Yes (Eligibility Code = 119)	N/A	N/A	N/A	N/A	N/A	Enter 90 day reconciliation period.	Individual is referred to sponsor. Individual enters into a 90 day reconciliation period.
DHS.13		Yes	Yes	No	No	Yes	N/A	N/A	N/A	N/A	Individual is verified as Legally present in Step 1.	Individual is verified as Legally present in Step 1 of the DHS service.
DHS.14		Yes	Yes	No	No	No	Yes	N/A	N/A	N/A	Individual is verified as Legally present in Step 2.	Individual is verified as Legally present in Step 2 of the DHS service.
DHS.15		Yes	Yes	No	No	No	No	Yes	Yes	Yes	Individual is a qualified non-citizen and cannot receive services for 5 years.	Individual is verified as Legally present in Step 3 of the DHS service. Individual is barred from receiving services for 5 years. The individual is a qualified non-citizen.
DHS.16		Yes	Yes	No	No	No	No	Yes	Yes	No	Individual is not a qualified non-citizen and cannot receive services for 5 years.	Individual is verified as Legally present in Step 3 of the DHS service. Individual is barred from receiving services for 5 years. The individual is not a qualified non-citizen.
DHS.17		Yes	Yes	No	No	No	No	Yes	No	Yes	Individual is a qualified non-citizen.	Individual is verified as Legally present in Step 3 of the DHS service. Individual is not barred for receiving services for 5 years and is a qualified non-citizen.
DHS.18		Yes	Yes	No	No	No	No	Yes	No	No	Individual is not a qualified non-citizen.	Individual is verified as Legally present in Step 3 of the DHS service. Individual is not barred for receiving services for 5 years and is not a qualified non-citizen.
DHS.19		Yes	Yes	No	No	No	No	Yes	Met	Yes	Individual has met the five year bar on services and is a qualified non-citizen.	Individual is verified as Legally present in Step 3 of the DHS service. Individual has met the 5 year bar and is a qualified non-citizen.
DHS.20		Yes	Yes	No	No	No	No	Yes	Met	No	Individual has met the five year bar on services and is not a qualified non-citizen.	Individual is verified as Legally present in Step 3 of the DHS service. Individual has met the 5 year bar and is not a qualified non-citizen.
DHS.21		Yes	Yes	No	No	No	No	No	N/A	N/A	Individual is verified as not Legally present.	Individual is verified as not Legally present after all 3 steps.
DHS.22		Yes	No (Eligibility Code = 37)	Yes (Eligibility Code = 32)	Yes (Eligibility Code = 119)	N/A	N/A	N/A	N/A	N/A	Enter 90 day reconciliation period.	The individual must correct certain data elements after a mismatch of data elements. The individual must resubmit with a SEVIS ID. Individual is referred to sponsor. Individual enters into a 90 day reconciliation period.
DHS.23		Yes	No (Eligibility Code = 37)	Yes (Eligibility Code = 32)	No	Yes	N/A	N/A	N/A	N/A	Individual is verified as Legally present in Step 1.	The individual must correct certain data elements after a mismatch of data elements. The individual must resubmit with a SEVIS ID. Individual is verified as Legally present in Step 1 of the DHS service.
DHS.24		Yes	No (Eligibility Code = 37)	Yes (Eligibility Code = 32)	No	No	Yes	N/A	N/A	N/A	Individual is verified as Legally present in Step 2.	The individual must correct certain data elements after a mismatch of data elements. The individual must resubmit with a SEVIS ID. Individual is verified as Legally present in Step 2 of the DHS service.
DHS.25		Yes	No (Eligibility Code = 37)	Yes (Eligibility Code = 32)	No	No	No	Yes	Yes	Yes	Individual is a qualified non-citizen and cannot receive services for 5 years.	The individual must correct certain data elements after a mismatch of data elements. The individual must resubmit with a SEVIS ID. Individual is verified as Legally present in Step 3 of the DHS service. Individual is barred from receiving services for 5 years. The individual is a qualified non-citizen.



A. Group #	B. Count	C. Eligible Documentation	D. Valid Request	E. SEVIS ID Required	F. Refer to Student/Visitor to Sponsor	G. Verification Match? (Step 1)	H. Verification Match (Step 2)	I. Verification Match (Step 3)	J. Five Year Bar?	K. Qualified Non-Citizen?	L. Outcome	M. Scenario Text
DHS.26		Yes	No (Eligibility Code = 37)	Yes (Eligibility Code = 32)	No	No	No	Yes	Yes	No	Individual is not a qualified non-citizen and cannot receive services for 5 years.	The individual must correct certain data elements after a mismatch of data elements. The individual must resubmit with a SEVIS ID. Individual is verified as Legally present in Step 3 of the DHS service. Individual is barred from receiving services for 5 years. The individual is not a qualified non-citizen.
DHS.27		Yes	No (Eligibility Code = 37)	Yes (Eligibility Code = 32)	No	No	No	Yes	No	Yes	Individual is a qualified non-citizen.	The individual must correct certain data elements after a mismatch of data elements. The individual must resubmit with a SEVIS ID. Individual is verified as Legally present in Step 3 of the DHS service. Individual is not barred for receiving services for 5 years and is a qualified non-citizen.
DHS.28		Yes	No (Eligibility Code = 37)	Yes (Eligibility Code = 32)	No	No	No	Yes	No	No	Individual is not a qualified non-citizen.	The individual must correct certain data elements after a mismatch of data elements. The individual must resubmit with a SEVIS ID. Individual is verified as Legally present in Step 3 of the DHS service. Individual is not barred for receiving services for 5 years and is not a qualified non-citizen.
DHS.29		Yes	No (Eligibility Code = 37)	Yes (Eligibility Code = 32)	No	No	No	Yes	Met	Yes	Individual has met the five year bar on services and is a qualified non-citizen.	The individual must correct certain data elements after a mismatch of data elements. The individual must resubmit with a SEVIS ID. Individual is verified as Legally present in Step 3 of the DHS service. Individual has met the 5 year bar and is a qualified non-citizen...
DHS.30		Yes	No (Eligibility Code = 37)	Yes (Eligibility Code = 32)	No	No	No	Yes	Met	No	Individual has met the five year bar on services and is not a qualified non-citizen.	The individual must correct certain data elements after a mismatch of data elements. The individual must resubmit with a SEVIS ID. Individual is verified as Legally present in Step 3 of the DHS service. Individual has met the 5 year bar and is not a qualified non-citizen.
DHS.31		Yes	No (Eligibility Code = 37)	Yes (Eligibility Code = 32)	No	No	No	No	N/A	N/A	Individual is verified as not Legally present.	The individual must correct certain data elements after a mismatch of data elements. The individual must resubmit with a SEVIS ID. Individual is verified as not Legally present after all 3 steps. Individual has met the 5 year bar and is not a qualified non-citizen.
DHS.32		Yes	No (Eligibility Code = 37)	No	Yes (Eligibility Code = 119)	N/A	N/A	N/A	N/A	N/A	Enter 90 day reconciliation period.	The individual must correct certain data elements after a mismatch of data elements. Individual is referred to sponsor. Individual enters into a 90 day reconciliation period.
DHS.33		Yes	No (Eligibility Code = 37)	No	No	Yes	N/A	N/A	N/A	N/A	Individual is verified as Legally present in Step 1.	The individual must correct certain data elements after a mismatch of data elements. Individual is verified as Legally present in Step 1 of the DHS service.
DHS.34		Yes	No (Eligibility Code = 37)	No	No	No	Yes	N/A	N/A	N/A	Individual is verified as Legally present in Step 2.	The individual must correct certain data elements after a mismatch of data elements. Individual is verified as Legally present in Step 2 of the DHS service.
DHS.35		Yes	No (Eligibility Code = 37)	No	No	No	No	Yes	Yes	Yes	Individual is a qualified non-citizen and cannot receive services for 5 years.	The individual must correct certain data elements after a mismatch of data elements. Individual is verified as Legally present in Step 3 of the DHS service. Individual is barred from receiving services for 5 years. The individual is a qualified non-citizen.
DHS.36		Yes	No (Eligibility Code = 37)	No	No	No	No	Yes	Yes	No	Individual is not a qualified non-citizen and cannot receive services for 5 years.	The individual must correct certain data elements after a mismatch of data elements. Individual is verified as Legally present in Step 3 of the DHS service. Individual is barred from receiving services for 5 years. The individual is not a qualified non-citizen.
DHS.37		Yes	No (Eligibility Code = 37)	No	No	No	No	Yes	No	Yes	Individual is a qualified non-citizen.	The individual must correct certain data elements after a mismatch of data elements. Individual is verified as Legally present in Step 3 of the DHS service. Individual is not barred for receiving services for 5 years and is a qualified non-citizen.
DHS.38		Yes	No (Eligibility Code = 37)	No	No	No	No	Yes	No	No	Individual is not a qualified non-citizen.	The individual must correct certain data elements after a mismatch of data elements. Individual is verified as Legally present in Step 3 of the DHS service. Individual is not barred for receiving services for 5 years and is not a qualified non-citizen.
DHS.39		Yes	No (Eligibility Code = 37)	No	No	No	No	Yes	Met	Yes	Individual has met the five year bar on services and is a qualified non-citizen.	The individual must correct certain data elements after a mismatch of data elements. Individual is verified as Legally present in Step 3 of the DHS service. Individual has met the 5 year bar and is a qualified non-citizen.
DHS.40		Yes	No (Eligibility Code = 37)	No	No	No	No	Yes	Met	No	Individual has met the five year bar on services and is not a qualified non-citizen.	The individual must correct certain data elements after a mismatch of data elements. Individual is verified as Legally present in Step 3 of the DHS service. Individual has met the 5 year bar and is not a qualified non-citizen.
DHS.41		Yes	No (Eligibility Code = 37)	No	No	No	No	No	N/A	N/A	Individual is verified as not Legally present.	The individual must correct certain data elements after a mismatch of data elements. Individual is verified as not Legally present after all 3 steps. Individual has met the 5 year bar and is not a qualified non-citizen.

## Appendix F Attachment 4: Application and Payload Characteristics

Table 1: Application Characteristics

NumberOfTaxHHs	NumberOfMedicaidHHs	RequestFinancialAid	HouseholdType	TaxFilingStatus	NumberOfDependents	PercentFPL
0 thru 3 Extra row for each tax HH with separate values for each for tax filing status, dependents and %FPL	1 thru 3	Yes No	Tax HH & Medicaid HH Medicaid HH Only	Married filing jointly Married filing separately Individual Non-filer	0 thru 20	0 thru greater than 400%
CitizenshipStatus	DisabilityStatus	Deceased	IncarcerationStatus	NonCustodialParent	FosterChildren	PregnancyNumberOfBabies
<i>Citizen</i> Non-citizen, lawfully present Non-citizen, not lawfully present (Add Negative Tests)	<i>Not Disabled</i> Disabled	<i>Not Deceased</i> Deceased	<i>Not Incarcerated</i> Incarcerated	<i>No</i> Yes	<i>No</i> Yes	<i>None (blank)</i> 1,2,3,4,5, etc.
ResidencyVerification	AgeLessThanOneYear	Age1To18Years	Age19_20_21Years	Age22To64Years	Age65OrMoreYears	AmericanIndianStatus
<i>No</i> Yes	<i>No</i> Yes	<i>No</i> Yes	<i>No</i> Yes	<i>No</i> Yes	<i>No</i> Yes	<i>No</i> Yes
FullTimeStudent	ChangeInEmployment					
<i>No</i> Yes	<i>No</i> Stopped working Decreased hours Changed job					

Table 2: Payload Index Schema

#	A. Master Inventory ID	B. Scenario	C. Payload ID	D. Application ID	E. Person ID*	F. Index
1.	H3	SSA1 Verified dead. Cannot enter Marketplace.	1 2 3 4	(appID)	(personID)	H3.SSA1.1.appID.personID H3.SSA1.2.appID.personID H3.SSA1.3.appID.personID H3.SSA1.4.appID.personID
2.	H3	SSA2 Verified incarcerated, citizen. Cannot enter Marketplace.	1 2 3 4	(appID)	(personID)	H3.SSA2.1.appID.personID H3.SSA2.2.appID.personID H3.SSA2.3.appID.personID H3.SSA2.4.appID.personID
3.	H3	SSA3 Verified citizen, not incarcerated. Can enter Marketplace.	1 2 3 4	(appID)	(personID)	H3.SSA3.1.appID.personID H3.SSA3.2.appID.personID H3.SSA3.3.appID.personID H3.SSA3.4.appID.personID
4.	H3	SSA4 Verified incarcerated, non-citizen. Cannot enter Marketplace.	1 2 3 4	(appID)	(personID)	H3.SSA4.1.appID.personID H3.SSA4.2.appID.personID H3.SSA4.3.appID.personID H3.SSA4.4.appID.personID
5.	H3	SSA5 Citizenship not verified. Need lawful presence verif.	1 2 3 4	(appID)	(personID)	H3.SSA5.1.appID.personID H3.SSA5.2.appID.personID H3.SSA5.3.appID.personID H3.SSA5.4.appID.personID
6.	H3	SSA6 DOB does not match SSN and name record. Need additional info.	1 2 3 4	(appID)	(personID)	H3.SSA6.1.appID.personID H3.SSA6.2.appID.personID H3.SSA6.3.appID.personID H3.SSA6.4.appID.personID

#	A. Master Inventory ID	B. Security	C. Payload ID	D. Application ID	E. Person ID*	F. Index
7.	H3	SSA7 Name and DOB do not match SSN record. Need additional info.	1 2 3 4	(applID)	(personID)	H3 SSA7.1 applID personID H3 SSA7.2 applID personID H3 SSA7.3 applID personID H3 SSA7.4 applID personID
8.	H3	SSA8 Name does not match SSN and DOB record. Need additional info.	1 2 3 4	(applID)	(personID)	H3 SSA8.1 applID personID H3 SSA8.2 applID personID H3 SSA8.3 applID personID H3 SSA8.4 applID personID
9.	H3	SSA9 SSN not verified. Need lawful presence verif.	1 2 3 4	(applID)	(personID)	H3 SSA9.1 applID personID H3 SSA9.2 applID personID H3 SSA9.3 applID personID H3 SSA9.4 applID personID

\*Note: Person ID will only be valuable for certain services in which multiple individuals are associated with one request.

DRAFT



## Appendix G Additional Notes

Additional notes were collected from the SSA Interagency Project Team (IPT) Meeting Minutes:

IPT Meeting Date	Topic	Discussion Notes
April 2, 2013	Testing Preparation	<ul style="list-style-type: none"><li>The consensus of the SSA IPT is that SSA and CMS can't perform any Interagency Testing at this moment.<ul style="list-style-type: none"><li><b>Suggestion:</b> For Release 5 testing, SSA and CMS could arrange to do the network testing first.</li><li>QSSI could do a network layer test, but would have to execute a firewall request, which would be performed in the IMP1 environment.</li><li>QSSI will initiate the network layer , then CMS will have to approve request and then the approval will be sent to Terremark.</li></ul></li></ul>
April 2, 2013	Error Handling	<ul style="list-style-type: none"><li>SSA reports that it will use 5 response codes.</li></ul>
April 9, 2013	Testing Schedule	<ul style="list-style-type: none"><li>SSA provided CMS its testing calendar with all of the SSA testing dates.</li><li>SSA has already started its own Internal Validation Testing.</li></ul>
April 16, 2013	End Point Information	<ul style="list-style-type: none"><li>SSA provided its IP Addresses to CMS during the week ending April 12, 2013.</li></ul>
April 23, 2013	Testing Schedule: Time Slicing	<ul style="list-style-type: none"><li>QSSI ACA Testing Team is meeting with each Federal Partner on a one-to-one basis in order to assure that the connection between the Federal Partner and CMS is working appropriately without any interruptions or blocks.</li></ul>
April 23, 2013	Schema Changes	<ul style="list-style-type: none"><li>SSA informed CMS that there are schema changes for Title II monthly optional applicant data, which will require a documentation change request to be introduced (CR).</li><li>The schema change could not be promoted since Release 5 ended in March 2013. August 2013 is the earliest that SSA could test Title II monthly income functionality with CMS. CMS could test everything except partial months in which Title II income is not available.</li></ul>
April 30, 2013	Service Level Agreements (SLA)	<ul style="list-style-type: none"><li>SSA received all of the relevant SLA files, and will review internally. CMS and SSA to schedule a meeting to further discuss and finalize the CMS-SSA SLA.</li></ul>
April 30, 2013	Firewall Request	<ul style="list-style-type: none"><li>The QSSI Development Team still does not have an update regarding the firewall request, and enlisted the assistance of CMS to expedite the request. CMS is waiting for the firewall request to be accepted.</li><li>Once Release 5 code hits the IMP1 environment, then CMS and SSA could perform the Application Layer testing.</li></ul>



## **Department of Health and Human Services**



**Centers for Medicare & Medicaid Services  
Center for Medicaid and CHIP Services**

# **Medicaid/CHIP and FFE State Engagement Summary**

**DRAFT**

**Version 1.0**

**July 30, 2012**

## Table of Contents

<b>1. Purpose.....</b>	<b>3</b>
<b>2. Process.....</b>	<b>3</b>
<b>3. Summary.....</b>	<b>4</b>
<b>4. Action Items/Next Steps: .....</b>	<b>5</b>
<b>Appendix.....</b>	<b>7</b>
a) Montana .....	7
b) Delaware .....	8
c) Wyoming.....	12
d) Arkansas.....	13
e) North Dakota.....	15

# 1. Purpose

CCIO, OIS and CMCS conducted outreach with five states that are likely to be an FFE state for 10/1/13 to gather feedback from State Medicaid and CHIP programs related to interaction with the federally facilitated exchange (FFE) and data service hub (DSH). The states selected to be part of this outreach effort included Delaware, Montana, Wyoming, Arkansas, and North Dakota. The hypothesis tested through these five calls is whether CMS' adopting a standard approach to the FFE and DSH builds, with a single definition of an electronic account for the FFE (including data taxonomy and use cases) and a prescribed interface with the DSH is both technically feasible and programmatically achievable for Medicaid/CHIP agencies. In other words, do the FFE and the DSH have to account for different state system capacities and business processes in their architecture?

# 2. Process

Each of the outreach meetings were supported by team members representing CCIO, OIS, and CMCS and their contractors and FFRDC. The agenda for each meeting was structured as follows:

- Introduction – Kirk Grothe and Jessica Kahn
- Overview of Hub & FFE – QSSI & CGI
  - Services Available
  - Consumption of Hub Services
- Interfacing with Medicaid/CHIP Agencies – Kirk Grothe/Mark Oh/Jessica Kahn/Benjamin Walker
  - Referrals for Eligibility/ Enrollment in Medicaid/CHIP
    - Interaction Model (Events/ Process/ Data)
    - Performance Standards
  - Referrals for QHP Enrollment from Medicaid/CHIP
  - QHP + Medicaid Flow within FFE

At the conclusion of each meeting, feedback was gathered and a summary document was created capturing the key points. Details of the five discussions are included in the Appendix and provide specific examples supporting the summarized feedback in the next section.

### 3. Summary

#### **States' feedback on Hub web services approach & their capacity to incorporate the data into workflows**

All were supportive of this approach and indicated a desire to have further discussions to learn more about how to interact with the FFE and Hub. Every state said they would have a role in receiving/providing content to CMS. What's different for each state is the level of capacity to accept file or consume a service, understanding of the mission, and level of maturity in its capacity to execute. It is clear that states need more detail from CMS to determine the level of complexity involved to support web services and the specific data which will be passed between states and CMS so that this can be accounted for in the workflows.

#### **States' feedback on the state/FFE interactions as described**

All the states are supportive of the state/FFE interaction as described and feel it is technically feasible. The states want to know what to build to and what specific data will be exchanged. Each state asked CMS for specifics on the FFE and DSH builds, including more detail about the Hub services and the electronic account transfers (content and use cases). Two states noted the potential value of the state noting the reason why an individual was not determined eligible (in an FFE assessment model), and perhaps even sharing the data the state used to verify eligibility (particularly current income). CMS will consider states' suggestions for additional services and requirements but has to consider what is feasible for Day 1 and still with a goal to have a standardized approach.

All of the states asked for definitions and data elements to understand what's in the web service. Nobody asked basic questions associated with this kind of hand-off, such as timing, business cycles, message sizes etc. Each state has its own frame of reference as to what it believes is its starting point for state/FFE interactions. However, states have not been provided a granular level of detail as to what the expected interactions look like, how they will be performed, and who is responsible for which activities. Presently CMS provides some of the technical specifications regarding services available within the service catalog via Centrasite. However, Centrasite does

not contain a full list. We need to articulate to the states what's available, the context, as well as how much more might be coming. Given the variability in states' potential system readiness, CMS is identifying alternative connection options based upon the state's system limitations.

#### **Can state send referrals for Potentially PTC-eligibles from Medicaid/CHIP to FFE/DSH?**

Very limited discussion took place on this topic due to limited time. However, the same transfer process is anticipated for sending accounts either direction for any of the defined interactions.

### **4. Action Items/Next Steps (\*key):**

- CMS should be clear on what services it will have available for day one operations, how it expects states to interoperate, and outline any assumptions it has for states\*
- CMS should graphically depict what data is being passed back and forth, how it is incorporated in to the workflow, and what the specifications are for the data being passed\*
- CMS need to provide more specifics on the FFE and DSH builds, including additional detail about the Hub services and specification, and the electronic account transfers (content and use cases); the on-boarding/readiness timeline and milestones by when state capacities need to be fully developed and operational, and by when CMS will have services ready for states to test. This includes defining an alternative path for the FFE to interact with states that cannot successfully exchange the electronic account, e.g. PDF applications.\*
- CMCS and OIS to ensure that each state has received Centrasite access and any documentation that is available/ready to share.
- Follow-up calls with each of the states once they've reviewed the information.
- CMS should provide a primary set of business scenarios to states so that all parties have a unified understanding of the context.
- A clear/concise communication plan that tells the whole interaction model is needed. CMS is currently referring people to PRAs and segmented documents.

## Appendix

A summary of the five state outreach calls is as follows:

### 1. Montana

- CCIIO/OIS to share/provide access to the service catalog and other artifacts helpful in understanding the services/options
- MT asked about how CMS will address the issue of duplicate applications and enrollments and if they would be expected to tell CMS if an electronic account sent to them was for an individual already enrolled in Medicaid or CHIP.
  - A discussion ensued about verifying existing enrollment in Medicaid/CHIP earlier in the FFE's process, possibly via a 270/271 transaction.
  - MT noted that this might introduce additional HIPAA consideration for the state, if so.
  - MT asked about how identification would occur for newborns without an SSN
  - It was noted that remote ID proofing process only applies to the application filer, not the whole household
- MT asked about the FFE verification plan and what data would be used to evaluate Medicaid/CHIP eligibility.
- Montana will give further consideration into the use of FFE/Hub, especially with regard to the determination vs. assessment option.
- The state validated the approach of a defined interface, defined hand-off use cases and defined electronic account data as technically feasible though deferred discussion of the impact on their business workflows, given their business staff were not present on the call.
- MT requested to receive all of the household's application information, even those with QHP/APTC eligibility findings to assess for other benefits/human services. A caseworker would take this information and go through the application workflow. While this may improve the overall consumer experience/outcomes, it would not align with the desire to minimize the number of interactions with the states.
- MT confirmed that they take attestation for residency

- CMS to schedule follow-up session to continue the discussion, with more policy-focused topics next time

## 2. Delaware

- DE asked about the data the FFE will be using for income (i.e. what are the date parameters (historical tax records vs. current income)
  - FFE will look at both, will start by moving towards APTC (i.e. historical tax records) until some indication that individual is potentially Medicaid eligible, then will shift to current income information as warranted.
    - FFE intends to check 3 data sources:
      - State quarterly wage data
      - SSA
      - Unemployment
      - Member must attest to other income
- DE asked whether FFE/DSH intended to ping DE sources in real time or store updated data
  - CMS indicated they wanted to discuss this further with the state as to how this could work, but understands that all states might not be the same.
- It was noted that DE had indicated that it currently has 26 local sources of income data.
  - CMS reps indicated that this might have an impact on whether DE would accept CMS results as assessment or determination
- CMS asked when DE needed to resolve this to support their decision-making timeframe
  - DE noted that it needed input by next Wednesday in order to support its decision timeline (note: this timeframe was being driven by both the blueprint application process and to support the requirements definition process for their IT system development).
  - CMS indicated that they hoped to have a call with DE next week, but that they probably wouldn't have final information/decision in time to support DE's needs.



- It was clarified that DE does not have to decide about assessment vs. determination for the blueprint. A formal process to notify CMCS will be established (e.g. a SPA or via MOU) for this.
- QSSI noted it would be providing the following Verification services:
  - SSN
  - Citizenship
  - Composite – lawful presence, SSN, DHS part 1
  - Expanded Lawful presence
  - Incarceration
  - Household Income
  - Current Income
  - APTC calculation
  - Account Transfer (both in and out)
- Data is currently in CentraSite
  - DE requested some assistance with Centrasite (i.e guide). CMS noted the upcoming webinar on Centrasite.
- QSSI still working on security wrapper for these services. CMCS will forward the ppt on security presented to the EI grantees.
- CMS asked whether its strategy to develop federal services with standard interface to single source for program (i.e. not to county level) would work with DE. CMS expounded upon this strategy by indicating that the account transfer is the key
  - DE indicated that this aligned with what is was expecting/planning for and that it was waiting for the service definition document, service description document, BSD and process flow diagrams. DE also noted that it has one point that handles both Medicaid and CHIP.
- OIS indicated that it was working on the account transfer BSD and would provide a draft in the next few days and hoped to solidify it by the end of the month (subject to feedback on the PRA for the data definitions in the application). Noted the need for deeper discussions on notifications. OIS indicated that this transfer needed to be looked at/walked through from both a systems perspective and a business perspective.
- DE contractor (Deloitte) asked three questions:

- Will the Hub data be point in time or will the data have a defined time period, potentially even retroactively?
- Would CMS be passing “trusted” or “verified” data or unverified data?
  - Response: yes some data would be verified, but might all pass other data such as “attested” data
- Would handoffs be in real-time or batch?
  - Response: yes – could be either
- DE asked whether it would be responsible for all verifications if it took FFE evaluation of Medicaid/CHIP eligibility as assessment.
- Response: DE would not be permitted to re-verify items previously verified by FFE. DE could perform additional verifications if the FFE is doing only assessments.
- DE asked whether CMS will provide listing/document stating what FFE will verify.
  - Response: will be provided soon
- CMS reiterated that it expected to use the same evaluation and verification criteria whether the state chose to use it as an assessment or a determination. Think that might result in need to state to do own verification might be something like Feds accept residency attestation while state wants to check other sources.
- CMS noted that it still has regulatory work to do on notifications, but envisions need for state specific information (such as the contract data for a state Medicaid call center) to be included in some notices
- DE noted that it had some things it needed to assess in making its decision on how to handle the assessment vs. determination question since it had some peculiar requirements that come from an old lawsuit (this was specific to notification language)
- CMS noted that it had published the streamlined application data elements in the federal register, feedback is due by September and a final decision due by Dec 31. DE noted that they knew of the fed register announcement, that the finalization was very late in its process and asked if CMS was interested in getting some earlier feedback on “gaps”
- CMS noted that it welcomed any early inputs
- Discussed Hypotheses of providing same information
- Questions came up on what does reject look like? Possible need for a reason code vs. data modification?

- CMS looking for information on what it would take
- It was noted that the effective date of coverage was not a data transfer issue.
- FFE to include an indication of the data timeframe
- CMS indicated that some states might be looking at using “reasonably projected income” to smooth transfers and that this might influence state decisions on whether to use federal input as assessment vs. determination. CMS noted that this topic is still in need of further discussion – no indication of whether it applied to DE
- DE asked for insights on how detailed the data parameters will be in the Service Catalog. CMS indicated that it will provide a draft of the account transfer BSD today that might clarify this. CMS noted that this is only a draft and might evolve (possibly due to changes from the streamlined application data PRA). CMS noted that DE might need both the BSD and the application data model
- DE asked how likely it would be that the data elements would change based upon PRA feedback. CMS indicated that it was too early to tell but that some data elements were likely set.
- DE was not concerned about accepting an electronic transfer from the FFE and incorporating the information into their workflow. The process of receiving transfers is aligned with the way they do things now. However they are very concerned about getting the information needed in order to define the requirements and create their system design in time to develop.
- DE asked how the information should be communicated when a state finds the applicant not eligible for Medicaid/CHIP, e.g. a reason code and possibly providing the additional data (e.g. a higher income level)
- Summary of items to be provided by CMS:
  - Account transfer BSD
  - Service definition document
  - Data flows (particularly for account transfer)
  - Business functional descriptions

### 3. Wyoming

- WY is in the process of building a new Integrated Eligibility System. WY currently has separate systems for Medicaid and CHIP but looks to integrate these into one eligibility system for both. WY expected to get into design work in SEP/OCT and have new system in place by October 2013. The new program currently will just be for Medicaid/CHIP, but WY expects to expand it in the future to include other human services programs.
- WY asked when it could see the FFE/DSH architectural model (since it wanted to use them to shape its design). WY currently using FTP/SFTP/HTTPS as interfaces but looking to go towards web services with new system. This is a significant jump.
- CMS noted it was developing service definitions including WSDL, data element descriptions (subject to PRA) and security wrappers. (Information on these is available on Centrasite). CMS noted that security details are “baked in” to the services. CMS noted that it will also be releasing some new MARS-E requirements shortly, but that these were already “baked in” as well.
- Reviewed scenario for 2 adult, 2 child family where one adult eligible for Medicaid and other eligible for APTC. Scenario involved FFE applying the federal rules and then transmitting information/transferring account (if Medicaid/CHIP appropriate) to state for the state to render its decision. It was noted that there is the potential for the state to need to do more than what is being done by FFE. CMS noted that the “operational context” (i.e. rule and procedures for the FFE) are still being worked out.
- WY asked what information would be needed from the state. CMS indicated it was still working out what would be expected from/provided to the state (e.g. handoffs).
- CMS indicated that it expected to use one process to evaluate eligibility for Medicaid/CHIP whether doing an “assessment” or a “determination”. Discussed the “assessment guardrails” where state can’t ask for same information again.
- Discussed whether WY wanted separate account transfers for Medicaid adult vs. children. WY said it assigns each individual their own master ID and then links the household together. Asked what information WY needed for APTC adult. WY not sure since currently working on exist business processes, but sounded like they needed the information so they could get complete picture of household income. WY indicated it really couldn’t answer this question yet. It may be able to do so once it finishes 1)

assessing current business processes and 2) determining what needs to be changed to comply with ACA/take advantage to the new system they are developing.

- WY did not see a problem with matching up to a federally provided eligibility service, but need the information on this interface from the CMS. CMS to provide WY with FFE/DSH thought process BSD (architecture?) and data model.
- WY was not ready to discuss how their new system would handle the family mentioned above if the family started with the state Medicaid system, since it is still working how out it will transform itself to meet the ACA.
- WY welcomed input on what it needs to know and asked for data as soon as possible since it would be starting design work in Sept/Oct. WY confirmed that they would be able to have their contractor (contract is still not awarded, raising concerns) build to meet up with federally provided specs.
- Reviewed other touch points, such as non ESI MEC coverage check of Medicaid//CHIP (via XML message) which WY can accommodate. Other state data sources – WY still assessing, just completed preliminary inventory, proceeding with more detailed inventory. Many WY systems are old so an API wrapper might be needed to be developed.
- Asked what DSH/FFE services WY wanted to tap – WY indicated it was too early to tell. Might be able to discuss in a month or two.
- Asked what WY's CHIP waiting period is. Response 30 days. Discussed possibility for exchange to provide interim coverage during the waiting period, but that account transfer would need to be closely coordinated. WY not ready to discuss yet.
- Confirmed that WY is intending for new system to be primary touch-point with the FFE and Hub.

#### **4. Arkansas**

- Arkansas provided a slide documenting their conceptual model of the FFE and Medicaid/CHIP interactions and more than 20 assumptions, having clearly done some preliminary thinking.
- AR is preparing to work with web services and accept an account transfer.

- FFE looking to perform federally required Medicaid assessments, but noted that states have latitude to tailor. FFE not currently planning to handle state specific tailoring. AR looking to have FFE evaluations accepted by the state as “determinations”. Expects to align state Medicaid system to perform “same” calculations (subject to review of federal verification plan)
- AR currently has integrated eligibility system – will take advantage of data passed/provided by HIX, but understand it may need to perform some additional checks for other (non-Medicaid/CHIP) human service programs. AR also indicated that they have some “waiver” programs that might allow for some additional enrollment (not discussed – but would expect this to be treated like non-MAGI qualification.) CMS may need to hold further discussions on this.
- AR will still need to deal with non-MAGI determinations
- AR expects to receive information on entire household from FFE as a part of referrals
- AR looks to use state hub for the following: Department of Motor Vehicles/Department of Corrections/Child support Enforcement/vital records. AR would like the FFE to draw upon data from ARFinds – Further discussions on this planned.
- AR looking to obtain access to same sources as FFE will use – CMS confirmed this should be the case.
- CMS noted it expects to pass along all data for account even if a “determination” is made.
- It was noted that system of record (HIX for insurance/Medicaid/CHIP for managed care) would be responsible for passing information to IRS.
- Discussed issues with determinations for people without any IRS filings as well as those where insufficient data might exist.
- CMS asked if the following hypothesis seemed reasonable for AR:  
“CMS building interaction assuming a “standardized” approach that the state would consume & integrate into”
  - AR response: Yes – They recognize that FFE will be passing “whole” package and will adapt accordingly
- AR planning to use expanded Medicaid (i.e. 133% FPL determination).
- AR plans to be able to consume (i.e. work with) web services.

- CMS noted that if it was not doing determination, it might pass some of the manual data collection to the state (provided it looked like individual was Medicaid/CHIP eligible?)
- Discussed need for follow-on meeting

## 5. North Dakota

- CMS asked whether it would make more sense to ND to have the FFE use a single standard for reasonable compatibility or accommodate states' different standards. ND replied that a standardized approach would be a benefit to ensure consistency whether someone applies via the FFE or the state.
- ND indicated that they are leaning towards taking the FFE evaluation as an assessment because of their access to more timely state sources of data, e.g. current income.
- ND is developing a system for local verification data, called eVerify, which will turn Job Service and UI data into real-time service requests where possible.
- ND asked several questions indicating concern about the consumer experience where a household is being assessed by the FFE and the state for different programs at the same time.
- CMS asked what information the state would need from us to better understand the FFE and Medicaid/CHIP handoffs and the potential impact on their current workflow: MAGI rules and technical specifications, the interaction models, and data elements.
- CMS is ensuring that ND staff have access to the CMS Services Repository so they can access the Services Catalog.
- CMS noted that other states have asked about being able to query for existing QHP/APTC enrollment but ND said they have not given sufficient analysis yet (sans access to the BSDs).
- CMS offered to have the follow-up conversation with them, after sending them a package of information, with another comparable State. Call participants agreed that Montana would be a good candidate so CMS will schedule that call. Follow-up discussions will also be held at MESC and ISM in late August.



- ND noted, and CMS agreed, that while the handoff touch-points appear to be fairly defined, it's the data elements in the electronic account that are still not finalized.
- CMS will send ND the CMS and AR conceptual models for the FFE and Medicaid/CHIP interactions for them to consider and then draft their own and send back to us for feedback and discussion.



## **Centers for Medicare and Medicaid Services**

# **Evaluation of the HEALTH INSURANCE EXCHANGE (HIX) System Security Plan; dated July 29, 2013; Version 1.6**

Reference SSP Template V3.2 and ARS V1.5

August 19, 2013

Elizabeth Brown  
ebrown@mitre.org  
703.983.1421

### **NOTICE**

This information was produced for the U.S. Government under Contract Number TIRNO-99-D-00005, and is subject to Federal Acquisition Regulation Clause 52.227-14, Rights in Data—General, Alt. II (JUN 1987), Alt. III (JUN 1987), and Alt. IV (JUN 1987). No use other than that granted to the U.S. Government, or to those acting on behalf of the U.S. Government under that Clause, is authorized without the express written permission of The MITRE Corporation. For further information, please contact The MITRE Corporation, Contracts Office, 7515 Colshire Drive, M/S N320, McLean, VA 22102-7508, (703) 883-6000.

The views, opinions, and/or findings contained in this report are those of The MITRE Corporation and should not be construed as official government position, policy, or decision unless so designated by other documentation.

This document was prepared for authorized distribution only. It has not been approved for public release.

© 2009, The MITRE Corporation. All Rights Reserved.

**MITRE**  
**McLean, VA**

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)



(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)



(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)



(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)



(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)



(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)



(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)



(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)



(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)



(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)



(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)



(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)



(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)



(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)



(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)



(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)



(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)



(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)



(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)



(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)



(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)



(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)



(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)



(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)



(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)



(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)



(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)



(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)



(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)



(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)



(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)



(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)



(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)



(b)(5)

(b)(5)

## CIISG/EISG Communication Plan

3 March 2013

### **Background:**

This document is a formal communication plan developed to guide communications between two Office of Information Systems (OIS) groups. The Consumer Information and Insurance Group (CIISG) and the Enterprise Information Security Group have common integration points that can be leveraged to create a comprehensive framework for establish effective communications.

### **1. Stakeholders**

- OIS Leadership – Tony Trenkle; Mark Hogle; Henry Chao; Teresa Fryer;
- EISG Group Director – Teresa Fryer
- EISG Division Directors – Mike Mellor; Frank Schreibman;
- EISG SOC – Mike Mellor; contract staff
- EISG Staff – Feds; contract staff
- EISG SCA Testing GTL – Jason King; Jessica Hoffman
- CIISG Group Director – Monique Outerbridge
- CIISG Division Directors – Mark Oh; Kirk Grothe; Dan Miller
- CIISG XOC – Walt Dill; Tom Schankweiler

- ISSO – Darrin Lyles; Kevin Warren; John Gordon;
- CCIIO ISO – Tom Schankweiler
- MITRE (SCA Test Team) – Milton Shomo; Jim Bielski; testers
- Contractors – Generic
- Business Owner – As assigned per application
- System Maintainer – As assigned per application
- TRB – Standing Membership; Jason A. attending for EISG
- RAMG – Assigned Contract Officer Representatives (COR)

## 2. Communication Schedule

Items in green are fairly well established, others need better integration

Type of Interaction	Output	Sender	Recipient	Purpose	Comments	Delivery Frequency
CFACTS	Tracking system	ISSO	EISG Staff	Used to track security artifacts, milestone dates, and security weaknesses (POAMS)	Updated by ISSOs or contractors, reviewed and approved by EISG	Monthly updates

Type of Interaction	Output	Sender	Recipient	Purpose	Comments	Delivery Frequency
SCA Testing	SCA Package	MITRE	EISG Staff ISSO	Independent Analysis of system security. Provides comprehensive analysis and list of security risks	EISG is GTL on contract	Three weeks following completion of SCA testing
Path to ATO Schedule	Schedule	MITRE ISO	SCA GTL ISO ISSO OIS Leadership	Supports SCA Testing interaction and shows upcoming schedule of activities	Schedule is sent and briefed to EISG GTL weekly. Due to rapidly changing environment schedule is subject to changes weekly	Weekly
ATO Letters	Memo	OIS Leadership	Business Owner System Maintainer	Memo approves or denies system to operate with accreditation from the agency CIO	Memo's have had short life-span, consider issuing three year ATO's	As Required
TRB	XLC briefings & COTS product briefings	System Maintainer	TRB	Allows technical leaders to review systems during their development life-cycle. Also allows for procurement of COTS products not on the approved software list	Briefing materials are stored at TRB site, no need to copy them to CFACTS.	As Scheduled
TRB Letter	Letter	TRB	Business Owner System Maintainer	Communicates TRB direction and approvals	Artifacts are stored at	As Required
Risk Dashboards	1. ISAs 2. SCA Testing 3. State Readiness 4. Cloud Monitoring	CIISG Group Director	OIS leadership	Provides insight into top security Issues and Risks List Actions, Accomplishments, Issues, Risks, as mapped to Tier 1-2 Critical Path milestones	Dashboards can be added or removed from list.	Weekly
FEPS Schedule	Master Project schedule maintained by CIISG Feds	CIISG PMO Office	OIS leadership	Communicates the entire FEPS project schedule	None	Weekly
EISG/CIISG integration meeting	Meeting minutes and integration schedule with progress	ISSO	EISG Grp Dir  EISG Div Dir	To schedule integration of EISG monitoring tools into the cloud environment	Incident response PenTesting, read access to etc.	Weekly

Type of Interaction	Output	Sender	Recipient	Purpose	Comments	Delivery Frequency
CIISG Ops Security Meeting	Tracker Spreadsheet	ISSO	EISG Staff	Workgroup meets to discuss progress of completing tasks and milestones associated with meeting operational security objectives	Security items for XOC, Terremark, URS, EISG integration, <b>NotRes</b> ans, federal items <b>P</b>	Weekly
Policy and Guidance reviews	Final Draft documents and comment log	ISSO CIISG Staff	EISG (bi-directional) ISSO	Allow for input into development of security policy and guidance being developed in support of ACA	EISG has Final Draft Reviewer role: Previously commented on MARS-E, Pre-SCA Risk Assessment template, & ISA templates	As Required
System Attestation	Submission Package	Business Owner ISSO	EISG Staff	Activity to confirm CFACTS contact information, system test dates, and POAMS are current. Also requires that 1/3 of all security controls are tested.	Annual requirement, Business Owner and System Maintainer must attest to	Yearly (May 2013)
XOC Security Team	Real-time security dashboards	XOC	EISG SOC	Dashboard of environment, summary data only, possible drill down.	Will not be on-line until June 2013. Login Id to secure web page	Daily
CMS SOC Alerts	E-Mail alerts from CISO Security Team	EISG	XOC	Alerts from US Cert	CIISG to respond to alerts if applicable to operational environment	As Required
Security Training	Training to ISSOs and CFACTS users	EISG	ISSO CIISG Staff	Users require role based training and EISG provides agency training to key staff supporting the security program	CIISG has been expanding contractor interaction in CFACTS and sending more individuals to training.	As Required
CISO Security Forums and Conferences	Security training for staff	EISG	ISSO CIISG Staff	EISG offers quarterly briefings and OIS offers training through the training office	CIISG and CCIO need to participate in more training opportunities. Maybe we could also offer presentations	As Offered
Procurements	SOW and Task Orders	CIISG	EISG, RAMG	Maximize procurements to benefit CIISG and EISG	Previously participated jointly in EIDM and RIDP	As Required

Table 1 – Communication Schedule

There are likely other Communication points that could be added to the above table

### 3. RACI Chart

#### *Responsible*

Those who do the work to achieve the task/role

#### *Accountable* (also approver or final approving authority)

The one ultimately answerable for the correct and thorough completion of the deliverable or task, and the one who delegates the work to those responsible.

#### *Consulted* (sometimes counsel)

Those whose opinions are sought, typically subject matter experts; and with whom there is two-way communication.

#### *Informed*

Those who are kept up-to-date on progress, often only on completion of the task or deliverable; and with whom there is just one-way communication.

Item	Business Owner	CCIO ISO	CIISG Division Director	CIISG ISSOs	CIISG Group Director	CIISG XOC	Contractors	EISG Division Directors	EISG Group Director	EISG SCA Testing GTL	EISG SOC	EISG Staff	MITRE (SCA Test Team)	OIS Leadership	RAMG	System Maintainer	TRB
ATO Letters	I	I	I	I	I			C				R		A		I	
CFACTS	A	C		R			R	I	I			R				I	
CIISG Ops Security Meeting		C		A	I		R	I				R					
CISO Security Forums and Conferences	I	I	I	I	I		I	R	A			R				I	
CMS SOC Alerts		I		I		I	I	A			R						
EISG/CIISG Integration meeting		A		R	I	C		I	I			R				I	
FEPS Schedule	C	C	C	C	A		R										
Path to ATO Schedule	I	A	I	C	I					C			R	I		I	
Policy and Guidance reviews	C	A	I	C	C		R					C					
Procurements	A	R	C	C	C			C	C			C			C	C	
Risk Dashboards	C	R	R	R	A		C		I					I		C	
SCA Testing	A	C	C	C	I			I		R			R				
Security Training	R	C	I	R	I			I	A								
System Attestation	A	C	C	R					C								
TRB Meeting/Consult	A	C	C	I			C		I								
TRB Letter	I	I	I	I	I		I		I					I		I	A
XOC Security Operations	I	R	I	C	A	R	C										



## CIISG Security Briefing

### 1.0 Introduction

On Monday, 9th April 2012, a meeting was held at 8:00 A.M. via teleconference.

Bi-Weekly Recurring Meeting for CIISG to brief OCISO on the status of CCIIO Security Program. Please forward this meeting invite to others as needed. A webinar and teleconference number will be provided for those participants who are not located at the Central Office

#### 1.1 Participants

The following personnel participated in the meeting.

<i>Present</i>	<i>Name</i>	<i>Organization</i>	<i>E-Mail</i>
X	Thomas Schankweiler	CMS	thomas.schankweiler@cms.hhs.gov
X	Kevin Warren	CMS	kevin.warren@cms.hhs.gov
X	Teresa Fryer	CMS	Teresa.Fryer@cms.hhs.gov
	Michael Mellor	CMS	Michael.Mellor@cms.hhs.gov
X	Monique Outerbridge	CMS	monique.outerbridge@cms.hhs.gov
X	Darrin Lyles	CMS	Darrin.Lyles@cms.hhs.gov
	Jane Kim	CMS	Jane.Kim@CMS.hhs.gov
	Jason King	CMS	Jason.King@cms.hhs.gov
	Al Lewis	MITRE	ajlewis@mitre.org
X	Kris Blais	SphereCom Enterprises, Inc.	kblais@spherecomenterprises.com
X	Dennis Cooper	SphereCom Enterprises, Inc.	Dcooper@spherecomenterprises.com

### 2.0 Discussion Points

1. Overview of this Briefing
2. Presentation
3. Questions for next session

## 2.1 Opening Remarks and Presentation

Tom Schankweiler: Essentially what I would like to do with these bi-weekly meetings is to sync up what CIISG is doing on behalf of CCIIO with the CISO office. This particular briefing is more security-centric.

## 2.2 Discussion

Tom Schankweiler: I've sent out a presentation last night, it should have April 2012 at the bottom. First order of business, I've noticed that this is not a good time slot for Monique and she asked that we select a different time for future meetings. Will try to find a better time we can get together.

Teresa Fryer: Okay

Tom Schankweiler: Will include a good call in number for future meetings. Mark Oh and the other folks are putting together a more program level briefing about the exchanges and the data services hub area. So is that also your expectations as well?

Teresa Fryer: Yes, Also before you begin, could you explain your responsibilities and duties as it relates to CCIIO and CIISG?

Tom Schankweiler: Yes, I've got lots of responsibilities.

- I've been serving as the CISO for all of the affordable care act systems. We just recently hired two more people since January so I'll be able to divide those ISO responsibilities out.
- In charge of putting the entire security program together for the federal exchange, data service hub and state exchanges.
- Also, in charge of getting the operational environment over at Terremark up and running as well.
- Security Liaison to CCIIO for all security questions and matters.

And so there are three very distinct efforts that are going on there.

Plus I've been trying to learn as much I can about the business aspect of the exchange as well as the data service hub. Some of the efforts that we lead turned out to be Enterprise level efforts. For instance I've started an effort around the identity management and ID proofing/Multi-factor authentication for the exchange work and it quickly morphed into an Enterprise level initiative. There was some level of effort for that going on for some of the non-exchange work.

But not around RFDP it was more of the EIDM and looking at it from a provider perspective. Most of the tools and applications bringing forward are now running through the TRB. There have been somewhat challenging me to ensure that things I'm bringing forward can be piloted in such a way that CMS as a whole can start to look forward to taking advantage of the lessons learned and determining if it's something we can use across the board.

For instance, I'm bringing in this NotResp tool after going through the TRB they were very interested in what NotResp can do and would like to look at potentially using that across the enterprise. Another example is how we are bringing in NotResp for the software code testing.

SphereCom Enterprises Inc.

Again they were interested and wanted us to come back and tell them what we are going to be doing with Fortify and what we can do with that across the enterprise.

Beyond that it's been about trying to schedule all of the security test and evaluations. Working with all the contractors that have been coming on-board to make sure they are up on how to use CFACTS to enter the data and work with the POA&Ms. I've been in on all the ST&E kickoffs, attending as many of those as I could. So that is kind of at a 10,000' level of what I've been doing over the last year and a half.

Teresa Fryer: Okay, Thanks.

Tom Schankweiler: I'd like to talk about an agenda going forward. Determine what information is good to have as a general briefing for those interested in the e-cloud infrastructure platform and what the general security profile is. On a bi-weekly basis giving what our status is and where we currently stand and how the pieces are fitting together.

I'm going to start at the top level and work my way down. I'd also like to talk about the security testing as well as the pre-assessment strategy. Let's move on to slide 3

Terremark security services global infrastructure protections. This is intended to show kind of what's available to us and gleaning from our infrastructure service. This infrastructure service is an aspect where it is intended to be a multi-tenant environment; it's intended to be hybrid community in the aspect that it is just serving Federal community cloud. We're sitting from an infrastructure perspective just with-in a federal area.

The advanced threat detection may change a little bit. The rest of it is all true, the other one I may take off is compliance scan. They (Terremark) are doing compliance scans against their infrastructure piece only but it's not a SCAP compliant scan so I think I'm going to remove their circle and remap the rest. I'm also going to take another pass at it to make sure I haven't missed anything else from what an infrastructure is meant to provide.

This gives a quick snapshot of what specifically the infrastructure is doing. The demarcation point on one side is their internet facing firewall ports and the other demarcation is internally to us is the Hypervisor. They have control of our devices all the way up and through to the Hypervisor. Most of the servers that we have are dedicated to CCIIO.

The Next slide talks about our platform as a service. This may morph a little bit over the next month or so. But on the left side you see yellow or green brackets. The yellow brackets are things we've ordered and they are on their way in but haven't been fully realized yet. The Green is what we currently have in place today and fully operational. So our firewall is in place with that we get manual reviews of firewall logs as well as the logs themselves going to an **Not Res** server that is located in the infrastructure today but not on the platform. Everything is in place at the next layer up. One thing that may change in the future where it says full DR capabilities in place I want to go back and annotate each of those services that are available.

We've also tested our backup solution on three different apps so our backup solution is working pretty well. I've been forcing most of the newer apps now to repeat the same COOP functions like

SphereCom Enterprises Inc.

doing a backup / restores. While that is important I'm looking for them to bring other kinds of tests to the table. That is something I've been working on as well with some of our app owners.

The next one down is Application security capabilities; is a little bit more of an expansion but it looks at the application layer. We have the 3<sup>rd</sup> party monitoring from Newstar coming in and that lets us know that the site is up and operational and not just by a ping reply. It does some log ins and checks functionality making sure the system is actually operating and responding to queries more so that just being live and responding to a ping. We're hoping to have some additional information what Newstar can bring to the table in future meetings. The next one is the web penetration testing.

Teresa Fryer: Do you have information on things when you review what you are going to bring on? It would be good information for us just to see what you are looking at.

Tom Schankweiler: I can get you some of that information. I'm working it to keep Mike as up to date as possible. I'll work to make sure that as we are doing our evaluations. I don't know if Newstar went through the PRB process or not or if that was something that was ordered outside.

Web penetration testing that is Appscan. Right now we pretty much just have CALT up and running there. The other one that is running there is healthcare.gov but we don't necessarily review those that is done by the department. Healthcare.gov is one of those applications that crosses over both of our realms as well as the department. It's a front door to the exchange in some ways as well as an information gathering place where individuals can go to get information about healthcare.gov. We're looking to have monthly penetration testing whenever we have a public facing URL.

The other piece that is in is VPN **NotResp** We have two factor on that now, when someone logs in they have to be an administrator and when they log in to the VPN they are asked to log in with **NotResp** I've been trying to keep the two factor for the administrative folks different from what we think we are going to be doing for our common use individuals coming in from the internet. When we bring in **NotResp** it will have the ability to put a front end log in page that will allow us to use our PIV cards or we can authenticate with a phone factor or any other federated identity we choose to use at some point in the future.

Once you VPN you come through the Firewall and the XML Gateway. We've ordered it to support our XML traffic that is inbound. It's racked and the engineers are looking at how we are going to funnel traffic through there and how we are going to use it for different applications. In the box down below in the XML Gateway there is privileged account management. I somewhat spoke on that with **NotResp** I've providing information on that to CISO office on that and Mike has had a pretty good review on that.

**NotResp** s next one down. Mike had an opportunity to look at that one and it went through the IRB and had a pretty good discussion (CISO office was represented). Database security monitoring, I am looking at a couple different tools for that; I'm not completely satisfied with what we are getting and am monitoring what we get out of **NotResp** for our database security monitoring and I'm not sure if that will be completely sufficient. Another option is **NotResp** which has abilities around database security and it's something I need to learn a little more about what it can offer to us. So if there are specific things you are interested in bringing in-house for Database security I'd be interested in having a follow discussion about that Teresa.

SphereCom Enterprises Inc.

Teresa Fryer: Okay, thanks

Tom Schankweiler: The Pointers off to the right side basically show where we think the application will provide coverage.

- **NotResp** covers all three
- The Security coded analysis is predominately application layer tool
- Database monitoring is at the data layer.

If there are other application security tools you think we should be adding, again I'd be interested in hearing your analysis of things and capabilities we should be adding out there.

Teresa Fryer: Right

Tom Schankweiler: So the next question is what is our integration with the CMS integration points are with the CMS OCISO.

We are actually touching base in a lot of areas:

- Vulnerability reporting
- Compliance reporting which is up and coming through **NotResp**
- Agency level oversight again will be a future capability once the backcall is in between the hall between Terremark and the BDC. I believe they are working on some LDAP stuff now and eventually we'll want to be able to hook your SOC in with the capability of viewing traffic at Terremark.
- Security control assessments are on-going.
- System accreditation are on-going;
- POA&Ms are on-going;
- Mike had mentioned you are looking to bring in some computer forensics capabilities here in 2012 so I'd like to open up some discussions around what that entails.
- Incident response and breach reporting.

This is where I see us touching base on a fairly regular basis where we have a regular interaction and I want to see if there is anything else we should be adding to this laundry list. Also, where we want to be focusing some of our time and attention towards enhancing our interactions around these areas.

Next slide we have a view of all the systems that we have in CFACTS and the ones we have targeted to join CFACTS with their current status is.

- Terremark infrastructure service which was accredited and that expires at the end of the year it's up for out of station process and we've been asked to take it through the fedramp.
- Platform CALT tool which is in the same bucket in that they expire at the end of the month and are looking for out of stations.
- RBIS just recently tested and is awaiting its accreditation letter. POA&Ms having gone into CFACTS and the testing team / ISO there has been starting to add the responses to it. Awaiting a letter of accreditation from the CISO for RBIS.
  - Note: Red text is intended by to show what is changed from bi-week to bi-week or where we have some action due between us as a point of interest.



SphereCom Enterprises Inc.

- HIOS is currently operating at Terremark but outside of our firewalls but in the Federal multi-tenant area. We will be migrating and standing up a new version of HIOS inside our firewall and moving to another platform called **NotResp**. We are going to also be re-accrediting HIOS and be re-labeled internally as HIOS-J.
- ERRP which runs out of FIPS at the datacenter, that one was accredited and expires at the end of the year in 2013
- PCIP is actually out at NFC (National Finance Center) and they are operating that in their web hosting portal and they have accredited it and we did a review last year on their system. We made some recommendations to the COTAR who made some changes to their contract language for 2012. Due in May to get back with NFC and do another due diligence review to see where we are at with the requested changes. There is a letter that is on file I believe with your office that shows all of the risks and findings that we found to PCIP to the business owner as well as the COTAR explaining that we have reviewed their system, & documentation and here is the Risk you are accepting as the business owner with recommendations to change in your next contract language. As well as any steps forward that should be considered. If another copy of that letter is needed I can certainly send that along.

Monique Outerbridge: Tom, can we do that remotely?

Tom Schankweiler: Yes;

- HYAD is housed at HHS cloud and we are looking to move that before the fall prior to September 1<sup>st</sup>. Targeting somewhere between June and July. Expecting this will change from a low to a moderate level in the move to the Terremark cloud.
- MIDAS is inbound for Terremark and started in Dev. ST&E is slated late 2012
- CERTS, has the backend and has two variations of testing with. MITRE to provide alternative ideas for testing. **NotResp** will also be used.
- Workflow management tool, adobe lifecycle currently in dev. Moving into implementation sometime in next few months. The new MITRE test team will schedule a test date for Adobe.
- Correspondence management system we believe it will be thunderhead although could be adobe lifecycle. Not currently decided
- Placeholder for XML data and Druple services;
- RBIS will be relabeled ERDE; and a new system coming up for financial management. These names are placeholders and have not been finalized and don't yet appear in CFACTS.
- VAMS, not operational as yet, implementation zone. Working on configuration now scheduling for testing soon.
- CMMI, which we had a meeting about last week. That is the bulk of the systems coming in.
- ACA Security Strategy; 80% through documenting what security will look like. Expecting 2012 April for award. Expect to expand the work with MITRE; I'll forward control matrix over to you.

Trying to streamline documentation and testing. MITRE to create Summary documents that point back to tools with area of focus. We do have training coming in for all these tools (Classroom and CBTs); Create a list of controls that are continuously monitored and what is to be done yearly to drive down the cost of a three year assessment.

Teresa Fryer: It's important to be clear with vendors what to test.

Tom Schankweiler: ACA Sec programs, risks and issues; Intended to be programmatic risks, Systems coming up faster than 3<sup>rd</sup> party testing can occur; we have actions in progress and are contracting for a dedicated MITRE test team for 2012/2013 timeframe. System is operational before ATO issue; working with CISO on how to document this. Also, PAAS is subject to constant change, although we have good change management around testing, firewall and testing before loading into VMs.

Roadmap items:

- Near term touch points:
- eCloud and how do we provide report to CISO;
- how to we have greater participation in multi-agency
- We do have some inter-agency work and some upcoming department lead initiatives.
- Future focus points?
  - Data tagging?
  - White hat pen test or green test?
  - Multi-channel communications;
  - How are we conducting state stage gate reviews?

Feel free to review the backup slides; these to be used for alternative delivery to different groups

Teresa Fryer: Very good briefing for the

Monique Outerbridge: good briefing overall. Teresa Fryer, do you think we need more details?

Teresa Fryer: No, although there is more clarity with relationship with CIISG and CIICO

Tom Schankweiler: POA&M Remediation person for CISO? Is it funded? Will recirculate letter on this topic as follow-up.

### 2.3 Closing Remarks

Tom Schankweiler: Will add 1 or 2 slides up front to focus on changes. Red text down below will be peppered in context. We will review changes in follow up meetings.

### 3.0 Action Items and Owners

Status	Action Item	Assigned To	Details
New	Reschedule this bi-weekly meeting to a more accessible timeslot	Tom Schankweiler	Find new time for this bi-weekly meeting series.
New	Re-circulate email inquiry about new POA&M resource Liaison for CISO	Tom Schankweiler	Re-spark discussion on new open spot.

**4.0 Next Meeting**

Friday, April 27, 2012 11:00 AM-12:00 PM

**5.0 Approval**

\_\_\_\_\_  
Thomas Schankweiler, ISSO

11 April 2012  
Date