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 Operations and Regulatory Affairs/Freedom of Information Group**
Refer to: Control Number 122020137058 and PIN C5ZP

5/1/2015

William F. Marshall
Judicial Watch
425 Third St., SW, Suite 800
Washington, DC 20024

Dear Mr. Marshall:

This is the fourth 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, forty-five pages are released in the entirety, seventy-four pages are released in part, and twenty are withheld in full. All of these pages are enclosed and have been bates numbered. Three have been intentionally blank.

Comprised within the seventy-five pages redacted in part, is either, 1. Within the scope of June 13, 2014 modification and considered responsive to your request or 2. Exempt from disclosure pursuant to the deliberative process privilege of exemption 5 or 3. Exempt from disclosure pursuant to Exemption 6.

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 Gilmore
Director
Freedom of Information Group

Enclosure (141 pages)

Message

**From:** hcgovwarroom@googlegroups.com [hcgovwarroom@googlegroups.com]
on behalf of Dave Merrill [dave.merrill@eglobaltech.com]
**Sent:** 11/11/2013 1:47:58 AM
**To:** Deepak Bhatta [dbhatta@qssinc.com]; Dohnalek, Danny NotResp NotResp Asplen, Suzanne W. (CMS/CPI) [Suzanne.Asplen@cms.hhs.gov]; Glenn D. (CMS/OIS) Radcliffe [glenn.radcliffe@cms.hhs.gov]; Damon L. (CMS/OIS) Underwood [Damon.Underwood@cms.hhs.gov]; Richard Speights [Richard.Speights@cms.hhs.gov]; David.Nelson NotResp NotResp KKIM NotResp NotResp Hutton, Robert [robert_hutton@optum.com]; Starry, Melissa A. (CMS/OIS) [Melissa.Starry@cms.hhs.gov]; Manik Naik [mnaik@qssinc.com]; Tara Piazza [piazza_tara@bah.com]; Nick Mistry [nick.mistry@eglobaltech.com]; monique.outerbridge NotResp NotResp Courtney Gleason [courtney.gleason@eglobaltech.com]; Clawson, Geraldine G [gclawson@verizon.com]; Venky Natarajan [vnatarajan@qssinc.com]; Deiman, Mike [mike_deiman@optum.com]; McEachron, Errol (CGI Federal) NotResp NotResp; Jack Fletcher [John.Fletcher@cms.hhs.gov]; stacey holden [Stacey.Holden@cms.hhs.gov]; Doug C. (CMS/OIS) Margush [douglas.margush@cms.hhs.gov]; Johnston, James (CMS/CMMI) [James.Johnston@cms.hhs.gov]; Marc Richardson [Marc.richardson@cms.hhs.gov]; CMS CIISG_EOC NotResp @cms.hhs.gov]; James Miles - US [james.miles@caci.com]; Timothy J. (CMS/OIS) Purcell [timothy.purcell@cms.hhs.gov]; Prashant Malladi [pmalladi@qssinc.com]; Tom (CMS/OIS) Birkmire [Tom.Birkmire@cms.hhs.gov]; Winthrop, Monica (CGI Federal) NotResp NotResp Steve Boschulte - US (sboschulte@caci.com) [sboschulte@caci.com]; Joseph Cruzjesu [joseph.cruzjesu@eglobaltech.com]; Feodorov, Ovidiu (Non-Membe NotResp NotResp; mark.oh NotResp NotResp Graham, Joseph L [joe.graham@optum.com]; Todd.Couts NotResp NotResp Northwood, Todd (CMS/OIS) [Todd.Northwood@cms.hhs.gov]; Reba R. (CMS/OIS) Cole [Reba.Cole@cms.hhs.gov]; Johnston, Alissa A [alissa.johnston@optum.com]; booth, jon NotResp NotResp; Akhtar.Zaman NotResp NotResp; Wass, Stephen (CGI Federal) NotResp Patel, Ketan NotResp NotResp @googlegroups.com; Tyrone (CMS/OIS) Thompson [tyrone.thompson2@cms.hhs.gov]; Brett Kingswell [kingswell_brett@bah.com]; kirk.grothe NotResp NotResp; Lynn Jones [lbjones@mitre.org]; Kane, David (CMS/OIS) [David.Kane@cms.hhs.gov]; Hung B. (CMS/OIS) Van [Hung.Van@cms.hhs.gov]; benjamin.walker NotResp NotResp Alethia C. (CMS/OIS) Wongus [Alethia.Wongus@cms.hhs.gov]; 'lstudevent@mitre.org' (lstudevent@mitre.org) [lstudevent@mitre.org]; Ramadani, Ahmad F (CGI Federal) NotResp NotResp; Michael Finkel [mfinkel@qssinc.com]; NotResp NotResp; Busse, Thomas H [thomas_h_busse@optum.com]; Jagadish Gangahanumaiah (jgangahanumaiah@qssinc.com) [jgangahanumaiah@qssinc.com]; Doug Greene [dgreene@redhat.com]; Paul Donohoe [Paul.Donohoe@cms.hhs.gov]; thomas.schankweiler@cms.hhs.gov (CMS/OIS) Schankweiler [thomas.schankweiler@cms.hhs.gov]; robert.knight@cgifederal.com; henry.chao NotResp NotResp; Gonzalez, Timothy J (CGI Federal) NotResp NotResp linda_kern@optum.com
**Subject:** [hc.gov war room] Re: MEETING: PROD Go/No go - Attachment for discussion

**Attachments**: ATT00001.htm; 20131110_Deployment_Review_Notes.pptx

Attached please find the results of tonight's production promotion call. The resulting vote was a "GO", the 7.0.1.15 release will be promoted to PROD tonight.

Thank you,

Dave Merrill
(m) (b)(6)

On Nov 10, 2013, at 7:00 PM, Deepak Bhatta <dbhatta@qssinc.com> wrote:

Dave,

On the presentation you might want to add CGI results in the TEST2 environment since they will be providing the results from that environment. IMP1A results will continued to be provided by ACA.

Thanks
Deepak

**Deepak Bhatta | QSSI** | www.qssinc.com
**ACA – FFM Testing**
10480 Little Patuxent Parkway, Suite 1100
Columbia, MD 21044
301-977-7884 X 112 | (b)(6) Cell

**From:** Dave Merrill [mailto:dave.merrill@eglobaltech.com]
**Sent:** Sunday, November 10, 2013 6:57 PM
**To:** Dohnalek, Danny; Asplen, Suzanne W. (CMS/CPI); Glenn D. (CMS/OIS) Radcliffe; Damon L. (CMS/OIS) Underwood; Richard Speights; Dave Nelson; Karlton Kim; Hutton, Robert; Starry, Melissa A. (CMS/OIS); Manik Naik; Tara Piazza; Nick Mistry; Monique Outerbridge; Courtney GleasonFWD; Clawson, Geraldine G; Venky Natarajan; Deiman, Mike; CGI Federal; Jack Fletcher; stacey holden; Doug C. (CMS/OIS) Margush; Johnston, James (CMS/CMMI); Marc Richardson; CMS CIISG_EOC; James Miles - US; Timothy Purcell_con; Prashant Malladi; Tom (CMS/OIS) Birkmire; <monica.winthrop@cgifederal.com>; Steve Boschulte - US (sboschulte@caci.com); Joseph Cruzjesu; Feodorov, Ovidiu (Non-Member); Oh Mark U. (CMS/OIS); Graham, Joseph L; Todd (CMS/OIS) Couts; Northwood, Todd (CMS/OIS); Reba R. (CMS/OIS) Cole; Johnston, Alissa A; Booth, Jon G. (CMS/OC); Akhtar Zaman; Wass, Stephen (CGI Federal); <monica.winthrop@cgifederal.com>; Patel, Ketan (CMS/OC); hcgovwarroom@googlegroups.com; Tyrone (CMS/OIS) Thompson; Brett Kingswell; Kirk Grothe; Lynn Jones; Kane, David (CMS/OIS); Hung B. (CMS/OIS) Van; Walker, Benjamin L. (CMS/CCIIO); Alethia Wongus; 'lstudevent@mitre.org' (lstudevent@mitre.org); Ramadani, Ahmad F (CGI Federal); Michael Finkel; CMS - EIDM CMS Team; Busse, Thomas H; Jagadish Gangahanumaiah; Doug Greene; Paul Donohoe;thomas.schankweiler@cms.hhs.gov (CMS/OIS) Schankweiler; robert.knight@cgifederal.com; Deepak Bhatta; Chao, Henry (CMS/OIS); Timothy J (CGI Federal) Gonzalez; linda_kern@optum.com
**Subject:** MEETING: PROD Go/No go - Attachment for discussion

**Attached is the GO/NO-GO review presentation for our call at 7 pm.**

Thanks,

Dave Merrill
(m (b)(6)



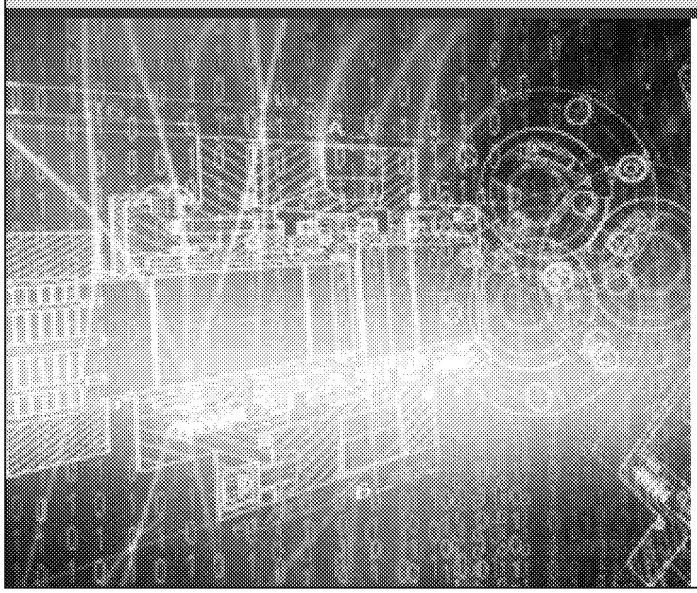
--

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.

---

CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES
OFFICE OF INFORMATION SERVICES

# Health Insurance Marketplace Deployment Review Package



*For:*

*FFM Release 7.0.1.15 Build #258*
*(Including fixes from 7.0.1.13,.14)*
*Promotion to Production during*
*Window 11/11/2013 1am – 5am*

*November 10, 2013*
*Version 2*

Environment Management Team – To Be Posted in CALT after Review.

# FFM to PROD Deployment Review: Maintenance Window 11/11 1:00 – 5:00 am

- ❑ **Roll Call**
- ❑ **Release Content**
  - ❑ Planned vs. Actual
- ❑ **Developer Checklist Review**
- ❑ **Fact Review**
  - ❑ Actual Scope (Build Notes) and Independent Tester Results
  - ❑ New Defect List
- ❑ **Risk Analysis Review**
- ❑ **Release Impact Assessment**
- ❑ **Promotion Decision**

## Roll Call

| Representative | Required (Primary) | Alternate | Attended |
|---|---|---|---|
| Approving Authority | Monique Outerbridge | Kirk Grothe | Monique Outerbridge, Kirk Grothe |
| Development | Mark Oh | Hung Van | Mark Oh |
| Testing | Akhtar Zaman | Richard Speights | Akhtar Zaman |
| PMO | Todd Couts | Tyrone Thompson | Todd Couts |
| Operations | Damon Underwood | Tom Birkmire | Tom Birkmire |
| System Integrator | Mike Finkel | | Mike Finkel |
| FFM Developer | Monica Winthrop | Errol McEahron | Errol McEahron |
| Independent Tester | Deepak Bhatta | Manik Naik | Deepak Bhatta, Manik Naik |
| Infrastructure | Doug Margush | Mark Oh | Mark Oh |
| Security | Tom Schankweiler | | Not Present |
| Environment Management | Jack Fletcher | | Jack Fletcher |
| Release Management | Stacey Holden | | Not Present |
| Change Control Board | Reba Cole | | Not Present |

## Release Content (Planned vs. Actual)

| Defect Fixes | Count |
|---|---|
| Scope | |
| Scoped from 7.0.1.13 | 14 |
| Scoped from 7.0.1.14 | 9 |
| Additions in 7.0.1.15 | 18 |
| Total Scope (Defect Fixes) | 41 |
| | |
| Defect Fixes Included in Build but failed Developer Testing | |
| Scoped from 7.0.1.13 | 5 |
| Scoped from 7.0.1.14 | 2 |
| Additions in 7.0.1.15 | 5 |
| Total Defect Fixes that failed Developer Testing | 12 |

**Sources:**
1. CGI November 10, 2013 Version 7.0.1.15 Build Notes for Build 258

# Development Release Package Checklist

Version Number: FFM 7.0.1.15 (Build 258)
Promotion Date/Time: Scheduled for Monday Nov. 11, 2013 01:00 – 05:00 am

Do the following items exist in CALT?

- ❑ Release Content (To Be Confirmed by CGI)
- ❑ Build Notes
- N/A Architecture Diagram
- N/A Systems Integration Diagram
- N/A Data Model/Schema/Architecture
- N/A BSD/XSD/ICDs **(CGI: Defect Fixes to align to existing doc.)**
- N/A Design Review Action Items/Response
- N/A Operations & Maintenance Manual **(Major Release, updated as necessary)**
- N/A Code Scan Reports **(Major Release Only)**
- ✓ Implementation Plan, Rollback Plan **(Checklist on Google Docs)**

Developer Representative: Errol McEahron
Checklist Captured by: Dave Merrill

## Fact Review

- ❑ Actual Scope (Build Notes) and Independent Tester Results
- ❑ New Defect List

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

(b)(5)

## Promotion Decision

| Voting Member | | Yes | No | Conditional |
|---|---|---|---|---|
| Development | Mark Oh | ✔ | | |
| Testing | Akhtar Zaman | ✔ | | |
| PMO | Todd Couts | ✔ | | |
| Operations | Tom Blrkmire | ✔ | | |
| FFM Developer | Errol | ✔ | | |
| Independent Tester | Manik Naik | ✔ | | |
| Security | Tom Schankweiler | | | |
| Approving Authority | Monique Outerbridge | ✔ | | |

Rationale:

(b)(5)

**Blank Page**

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**: CMSHIM_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 goin 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: (b)(6)
Customer Support: 800.314.0147 | 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>
**Date:** Thursday, August 1, 2013 10:55 AM
**To:** Jon Booth <jon.booth@cms.hhs.gov>, Ketan Patel BB <Ketan.Patel@cms.hhs.gov>, Bobbie Browning <Bobbie.Browning@govdelivery.com>
**Cc:** "Wright, Ltanya D. (CMS/OC)" <Ltanya.Wright@cms.hhs.gov>, Danielle Harris BB <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

**From:** <Booth>, "Jon G. (CMS/OC)" <Jon.Booth@cms.hhs.gov>
**Date:** Thursday, August 1, 2013 9:52 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, 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>
**Date:** Thursday, August 1, 2013 10:50 AM
**To:** Jon Booth <jon.booth@cms.hhs.gov>, Ketan Patel BB <Ketan.Patel@cms.hhs.gov>, Bobbie Browning <Bobbie.Browning@govdelivery.com>
**Cc:** "Wright, Ltanya D. (CMS/OC)" <Ltanya.Wright@cms.hhs.gov>, Danielle Harris BB <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

**From:** <Booth>, "Jon G. (CMS/OC)" <Jon.Booth@cms.hhs.gov>
**Date:** Thursday, August 1, 2013 9:22 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. To your 3rd point, does this mean API calls need to be modified or is this automatic?

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

**From:** Torleiv Flatebo <tor.flatebo@govdelivery.com>
**Date:** Thursday, August 1, 2013 9:00 AM
**To:** "Booth, Jon G. (CMS/OC)" <Jon.Booth@cms.hhs.gov>, "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.

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

**From:** <Booth>, "Jon G. (CMS/OC)" <Jon.Booth@cms.hhs.gov>
**Date:** Thursday, August 1, 2013 8:53 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.

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>
**Date:** Wednesday, July 31, 2013 5:56 PM
**To:** Ketan Patel BB <Ketan.Patel@cms.hhs.gov>, Bobbie Browning <Bobbie.Browning@govdelivery.com>
**Cc:** Jon Booth <jon.booth@cms.hhs.gov>, "Wright, Ltanya D. (CMS/OC)" <Ltanya.Wright@cms.hhs.gov>, Danielle Harris BB <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

**From:** Torleiv Flatebo <tor.flatebo@govdelivery.com>
**Date:** Wednesday, July 31, 2013 10:09 AM
**To:** "Patel, Ketan (CMS/OC)" <Ketan.Patel@cms.hhs.gov>, Bobbie Browning <Bobbie.Browning@govdelivery.com>
**Cc:** "Booth, Jon G. (CMS/OC)" <Jon.Booth@cms.hhs.gov>, "Wright, Ltanya D. (CMS/OC)" <Ltanya.Wright@cms.hhs.gov>, "Harris, Danielle Y. (CMS/OC)" <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

Customer Support: 800.314.0147 | help@govdelivery.com

**From:** <Patel>, "Ketan (CMS/OC)" <Ketan.Patel@cms.hhs.gov>
**Date:** Wednesday, July 31, 2013 10:04 AM
**To:** Torleiv Flatebo <tor.flatebo@govdelivery.com>, Bobbie Browning <Bobbie.Browning@govdelivery.com>
**Cc:** "Booth, Jon G. (CMS/OC)" <Jon.Booth@cms.hhs.gov>, "Wright, Ltanya D. (CMS/OC)" <Ltanya.Wright@cms.hhs.gov>, "Harris, Danielle Y. (CMS/OC)" <Danielle.Harris@cms.hhs.gov>
**Subject:** Re: TMS emails.

See attached hotmail recent example.

**From:** Tor Flatebo <Tor.Flatebo@govdelivery.com>
**Date:** Tuesday, July 30, 2013 5:50 PM
**To:** Ketan PATEL <ketan.patel@cms.hhs.gov>, Bobbie Browning <Bobbie.Browning@govdelivery.com>
**Cc:** Jon Booth BB <Jon.Booth@cms.hhs.gov>, Ltanya Wright <LTANYA.WRIGHT@CMS.HHS.GOV>, "HARRIS, (CMS/OBIS)" <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

**From:** <Patel>, "Ketan (CMS/OC)" <Ketan.Patel@cms.hhs.gov>
**Date:** Monday, July 29, 2013 2:35 PM

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

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

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

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

**To:** Bobbie Browning <Bobbie.Browning@govdelivery.com>, Torleiv Flatebo <tor.flatebo@govdelivery.com>

**Cc:** "Booth, Jon G. (CMS/OC)" <Jon.Booth@cms.hhs.gov>, "Wright, Ltanya D. (CMS/OC)" <Ltanya.Wright@cms.hhs.gov>, "Harris, Danielle Y. (CMS/OC)" <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**: Schankweiler, Thomas W. (CMS/OIS) [thomas.schankweiler@cms.hhs.gov]
**Sent**: 8/6/2013 12:16:57 PM
**To**: Booth, Jon G. (CMS/OC NotResp
**CC**: Willard, Adam (CMS/CTR) NotResp
NotResp hurston, Robert (CMS/CTR)
NotResp ; Oh, Mark U. (CMS/OIS)
NotResp
**Subject**: RE: odlinks for healthcare.gov

John,

In regards to the connection to GovDelivery can that be setup to use SSL? See note from Adam below.

Tom

**From:** Adam Willard [mailto:awillard@foregroundsecurity.com]
**Sent:** Tuesday, August 06, 2013 8:05 AM
**To:** Schankweiler, Thomas W. (CMS/OIS)
**Subject:** odlinks for healthcare.gov

It seems that the link for confirming your account is http and simple base64

https://hixpp.cms.gov/marketplace/global/en_US/emailVerification?trackingId NotResp
but
the underlying hyperlink was:
http://odlinks.govdelivery.com/track?type=click&enid NotResp
NotResp

the endid parameter of

NotResp

is
mailingid= NotResp
NotResp

**Adam Willard** (Contractor)
703-354-2229 x513 (Direct)
(b)(6) (Mobile)
Adam.Willard@cms.hhs.gov

**CMS XOC Security Team**
Consumer Information & Insurance Systems Group (CIISG)
Centers for Medicare & Medicaid Services (CMS)
703-594-4961/703-910-3993
ciisg-soc@cms.hhs.gov

Message

**From**: Schankweiler, Thomas W. (CMS/OIS) [thomas.schankweiler@cms.hhs.gov]
**Sent**: 8/6/2013 12:16:57 PM
**To**: Booth, Jon G. (CMS/OC) NotResp
**CC**: Willard, Adam (CMS/CTR) NotResp NotResp Thurston, Robert (CMS/CTR) NotResp ]; Oh, Mark U. (CMS/OIS) NotResp
**Subject**: RE: odlinks for healthcare.gov

John,

In regards to the connection to GovDelivery can that be setup to use SSL? See note from Adam below.

Tom

**From:** Adam Willard [mailto:awillard@foregroundsecurity.com]
**Sent:** Tuesday, August 06, 2013 8:05 AM
**To:** Schankweiler, Thomas W. (CMS/OIS)
**Subject:** odlinks for healthcare.gov

It seems that the link for confirming your account is http and simple base64

https://hixpp.cms.gov/marketplace/global/en_US/emailVerification?trackingId= NotResp
but
the underlying hyperlink was:
http://odlinks.govdelivery.com/track?type=click&enid= NotResp NotResp
the endid parameter of NotResp
is
mailingid: NotResp NotResp

**Adam Willard** (Contractor)
703-354-2229 x513 (Direct)
(b)(6) (Mobile)
Adam.Willard@cms.hhs.gov

**CMS XOC Security Team**
Consumer Information & Insurance Systems Group (CIISG)
Centers for Medicare & Medicaid Services (CMS)
703-594-4961/703-910-3993
ciisg-soc@cms.hhs.gov

Message

**From:** Schankweiler, Thomas W. (CMS/OIS) NotResp NotResp
**Sent:** 5/4/2012 1:32:13 AM
**To:** Miller, Daniel J. (CMS/OIS) NotResp NotResp
**CC:** Oh, Mark U. (CMS/OIS) NotResp NotResp Goswami, Mayank (CGI Federal) [Mayank.Goswami@cgifederal.com]
**Subject:** NotResp
**Attachments:** CMS Technical Reference Architecture Response.docx

Dan,

Here you go. I was able to answer every question except the last one. Some will probably require a little bit more explanation which I can try to provide on Friday, or we can setup a 30 minute session next week on a webinar to go over it with Steve.

Thanks,

Tom

---

**From:** Miller, Daniel J. (CMS/OIS)
**Sent:** Tuesday, May 01, 2012 1:57 PM
**To:** Schankweiler, Thomas W. (CMS/OIS)
**Cc:** Oh, Mark U. (CMS/OIS); Goswami, Mayank (CGI Federal)
**Subject:** FW: Security questions and concerns

Hi Tom, could you or one of your team members review the below and give us your best estimates on the responses? Mark and I (and Mayank from CGI so copying both) will be meeting with NAIC on Friday to launch the process by which they will take on and consume our FFE code to build out their SERFF system. They would like to get more understanding on the security requirements after reviewing what we sent them. Below they ask questions around whether SERFF would then need a separate ATO as a non-Fed third party, and whether the lack of FTI data in their side prevents some of the documents from having to be created (we're only looking at the specific section of functionality around Plan Management data). Also if any of the documents they reference are in fact required that they don't already have can you forward along?

**From:** Miller, Daniel J. (CMS/OIS)
**Sent:** Tuesday, May 01, 2012 1:52 PM
**To:** 'Chrisman, Kim K.'
**Cc:** Anderson, Steve W.; Kieras, Bridget; Neff, Clayton; Westphal, Tavis; Morrison, Joy E.; Oh, Mark U. (CMS/OIS)
**Subject:** RE: Security questions and concerns

Thanks Kim and Steve, let me send these to our security team to help respond before or during Friday.

**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



---

-----Original Message-----
From: Chrisman, Kim K. [mailto:KChrisman@naic.org]
Sent: Tuesday, May 01, 2012 1:46 PM
To: Miller, Daniel J. (CMS/OIS)
Cc: Anderson, Steve W.; Kieras, Bridget; Neff, Clayton; Westphal, Tavis; Morrison, Joy E.
Subject: Security questions and concerns

Dan, below are some security questions that Steve developed after reading the security information that was passed along. Our hope is that you/your team will be able to answer these questions either before you get to Kanas City or while you are here.

Kim Chrisman
SERFF Sr. Manager I Product Development
816-783-8590

All documentation gave us insight into the construction and security of the FFE and will be very helpful to our project. NAIC has the following statements and questions.

CMS Technical Reference Architecture - Minimum Security Guidance for States Supplement
(CMS TRA Minimum Security Guidance for States Draft v 0 8 _06082011.pdf)
* Does NAIC need to complete an Exchange Information Security Risk Assessment (RA)? If yes, we need the document.
* Does NAIC need to get an Authority To Operate (ATO) in order to do Plan Management?

SYSTEM SECURITY PLAN (SSP) PROCEDURE For State Exchanges
(ACA_SSP_Procedures_Final Draft V_0 99_040912.docx)
* Please confirm that NAIC does complete this document.
* Since SERFF doesn't handle Federal Tax Information (FTI), do we skip sections dealing with FTI?

Moderate Security Requirements SSP Workbook for Health Insurance Exchanges
(ACA_SSP_Attch_1_Workbook_Final Draft V_0 99_040912_.docx)
* Please confirm that NAIC does complete this document.
* Since SERFF doesn't handle Federal Tax Information (FTI), do we skip sections dealing with FTI?
* Some controls like VoIP we can't meet, is that evaluated in the Risk Assessment document?

Internal Revenue Service (IRS) Affordable Care Act (ACA) Safeguard Procedures Report (SPR)
(ACA_SSP_Attch_2_SPR_Template_Final Draft V_0.99_030512.doc)
* SERFF will not contain FTI data.

* Please confirm that NAIC does not complete this document.

System Security Plan (SSP) Template
(ACA_SSP_Template_Final Draft V_0 99_040912.doc)
* This document looks like the template for SYSTEM SECURITY PLAN (SSP) PROCEDURE For State Exchanges and Moderate Security Requirements SSP Workbook for Health Insurance Exchanges.
* Is CMS planning on replacing these two documents above with an SSP for just plan management?
* Would CMS create a RA for just plan management?

CMS Technical Reference Architecture - Java EE Application Development Guidelines Supplement
(CMS TRA_Java EE AppDvGdlnsSupp_v1.01_01082010.pdf)

Binary Data in XML
Standards for embedding binary data in XML are still being defined; CMS will publish the standards in a later revision of this document.

* Has CMS published a standard on transferring binary data?

* We did not find in any of these documents details on the security for web services.
* During our visit, Mark made reference to WS-Security with client-side certificates and SAML assertions. Please provide any documentation on securing web services.

---

.

CMS Technical Reference Architecture - Minimum Security Guidance for States Supplement (CMS TRA Minimum Security Guidance for States Draft v 0 8 _06082011.pdf)

*** Does NAIC need to complete an Exchange Information Security Risk Assessment (RA)? If yes, we need the document.**

Yes the templates are on CALT and can be provided in a zip file.

*** Does NAIC need to get an Authority To Operate (ATO) in order to do Plan Management?**

No, you will be issued an Authority to Connect (ATC) by CMS. However, someone in your organization will have to provide some sort of attestation to the security posture, typically this is someone at the C-Level like a CIO.

*** SYSTEM SECURITY PLAN (SSP) PROCEDURE For State Exchanges (ACA_SSP_Procedures_Final Draft V_0 99_040912.docx)**
**Please confirm that NAIC does complete this document.**
Yes, it is required.

*** Since SERFF doesn't handle Federal Tax Information (FTI), do we skip sections dealing with FTI?**

You do not need to complete the Safeguard Procedure Workbook (SPR), but inside the SSP you do need to meet the minimum controls identified.

**Moderate Security Requirements SSP Workbook for Health Insurance Exchanges (ACA_SSP_Attch_1_Workbook_Final Draft V_0 99_040912_.docx)**
*** Please confirm that NAIC does complete this document.**

Yes, it is required.

*** Since SERFF doesn't handle Federal Tax Information (FTI), do we skip sections dealing with FTI?**

Inside the SSP you do need to meet the minimum controls identified, you don't need to meet the more restrictive requirements identified as "For FTI".

*** Some controls like VoIP we can't meet, is that evaluated in the Risk Assessment document?**
**Internal Revenue Service (IRS) Affordable Care Act (ACA) Safeguard Procedures Report (SPR)**
**(ACA_SSP_Attch_2_SPR_Template_Final Draft V_0.99_030512.doc)**

No, since that is an IRS requirement only you will not need to meet it.

*** SERFF will not contain FTI data.**
*** Please confirm that NAIC does not complete this document.**
**System Security Plan (SSP) Template**
**(ACA_SSP_Template_Final Draft V_0 99_040912.doc)**

Yes the SSP template is required.

*** This document looks like the template for SYSTEM SECURITY PLAN (SSP) PROCEDURE For State Exchanges and Moderate Security Requirements SSP Workbook for Health Insurance Exchanges. Is CMS planning on replacing these two documents above with an SSP for just plan management?**

The minimum security controls need to be met for any system that interconnects with an Exchange

*** Would CMS create a RA for just plan management?**

The RA templates is a tool that allows you to document your risk, it is not function or application specific.

**CMS Technical Reference Architecture - Java EE Application Development Guidelines Supplement (CMS TRA_Java EE AppDvGdlnsSupp_v1.01_01082010.pdf)**
**Binary Data in XML**
**Standards for embedding binary data in XML are still being defined; CMS will publish the standards in a later revision of this document.**
*** Has CMS published a standard on transferring binary data?**
*** We did not find in any of these documents details on the security for web services.**
*** During our visit, Mark made reference to WS-Security with client-side certificates and SAML assertions. Please provide any documentation on securing web services.**

CMS will review and provide an update soon.

Message

**From:** Fryer, Teresa M. (CMS/OIS) NotResp NotResp

**Sent:** 12/2/2013 5:16:48 PM

**To:** Aronson, Lauren (CMS/OL) NotResp NotResp Schankweiler, Thomas W. (CMS/OIS) NotResp NotResp Boulanger, Jennifer L. (CMS) NotResp Linares, George E. (CMS/OIS) NotResp

**CC:** Nelson, David J. (CMS/OEM) NotResp NotResp Clark, Apryl C. (CMS/OL) NotResp NotResp Unruh, Patti (CMS/OC) NotResp NotResp Blum, Jonathan D. (CMS/CM NotResp NotResp

**Subject:** RE: URGENT -- Need review and comments ASAP

**Attachments:** SecurityandPrivacy-12-1-13 jb_tmf edits.docx

Here are my edits/comments.

Teresa

**From:** Aronson, Lauren (CMS/OL)
**Sent:** Monday, December 02, 2013 12:05 PM
**To:** Fryer, Teresa M. (CMS/OIS); Schankweiler, Thomas W. (CMS/OIS); Boulanger, Jennifer L. (CMS); Linares, George E. (CMS/OIS)
**Cc:** Nelson, David J. (CMS/OEM); Clark, Apryl C. (CMS/OL); Unruh, Patti (CMS/OC); Blum, Jonathan D. (CMS/CM)
**Subject:** RE: URGENT -- Need review and comments ASAP

Wonderful. Thank you so much. Any sense of timing? Would just help manage folks if we can give them an ETA. Thanks again!

**From:** Fryer, Teresa M. (CMS/OIS)
**Sent:** Monday, December 02, 2013 12:03 PM
**To:** Aronson, Lauren (CMS/OL); Schankweiler, Thomas W. (CMS/OIS); Boulanger, Jennifer L. (CMS); Linares, George E. (CMS/OIS)
**Cc:** Nelson, David J. (CMS/OEM); Clark, Apryl C. (CMS/OL); Unruh, Patti (CMS/OC); Blum, Jonathan D. (CMS/CM)
**Subject:** RE: URGENT -- Need review and comments ASAP

Yes, I have plenty and I have been working on them since this morning.

**From:** Aronson, Lauren (CMS/OL)
**Sent:** Monday, December 02, 2013 12:03 PM
**To:** Schankweiler, Thomas W. (CMS/OIS); Boulanger, Jennifer L. (CMS); Fryer, Teresa M. (CMS/OIS); Linares, George E. (CMS/OIS)
**Cc:** Nelson, David J. (CMS/OEM); Clark, Apryl C. (CMS/OL); Unruh, Patti (CMS/OC); Blum, Jonathan D. (CMS/CM)
**Subject:** RE: URGENT -- Need review and comments ASAP

Thank you so much.

Teresa/George/Dave - Other thoughts/edits? As jen mentioned we need edits asap. thank you

**From:** Schankweiler, Thomas W. (CMS/OIS)
**Sent:** Monday, December 02, 2013 11:12 AM
**To:** Boulanger, Jennifer L. (CMS); Fryer, Teresa M. (CMS/OIS); Linares, George E. (CMS/OIS)
**Cc:** Nelson, David J. (CMS/OEM); Aronson, Lauren (CMS/OL); Clark, Apryl C. (CMS/OL); Unruh, Patti (CMS/OC)
**Subject:** RE: URGENT -- Need review and comments ASAP

All,

I have edited as requested. Track Changes were enabled.

Thanks,

Tom

**From:** Boulanger, Jennifer L. (CMS)
**Sent:** Sunday, December 01, 2013 11:16 PM
**To:** Fryer, Teresa M. (CMS/OIS); Schankweiler, Thomas W. (CMS/OIS); Linares, George E. (CMS/OIS)
**Cc:** Nelson, David J. (CMS/OEM); Aronson, Lauren (CMS/OL); Clark, Apryl C. (CMS/OL); Unruh, Patti (CMS/OC)
**Subject:** RE: URGENT -- Need review and comments ASAP
**Importance:** High

I just received the word version of what is below. It should be easier to edit. Please send all edits back to Patti, Apryl and me as soon as you can. If we need a call to discuss, let us know asap. Thank you all very much and I apologize for the incredibly short time frame.

**From:** Boulanger, Jennifer L. (CMS)
**Sent:** Sunday, December 01, 2013 10:53 PM
**To:** Fryer, Teresa M. (CMS/OIS); Schankweiler, Thomas W. (CMS/OIS); Linares, George E. (CMS/OIS)
**Cc:** Nelson, David J. (CMS/OEM); Aronson, Lauren (CMS/OL); Clark, Apryl C. (CMS/OL); Unruh, Patti (CMS/OC)
**Subject:** URGENT -- Need review and comments ASAP
**Importance:** High

All – ASPA is working on statements that can be used if reporters call about the Mitre documents that we anticipate will be released to the press. This is an internal document and cannot be forwarded outside CMS.

Please review the statements below and send Patti Unruh, Apryl Clark and me your comments, corrections, additions first thing in the morning. Tom, George or I will call first thing to catch you up on what is going on. I have added some comments/questions in the document below in blue brackets.

Thank you for your help,

Jennifer

**From:** Friedman, Jennifer (OS/ASPA)
**Sent:** Sunday, December 01, 2013 10:19 PM

**To:** Boulanger, Jennifer L. (CMS); Unruh, Patti (CMS/OC)
**Cc:** O'Connor, Jen (OS/OGC); Flamberg, Gemma (HHS/OGC); Blackwood, Kristine (HHS/ASL); Scott, Meghan (HHS/ASL)
**Subject:** For review- follow-up from call

Hi Jennifer and Patti,

Following up on our call re: security today, below are some draft statements and Q/A for CMS review and approval. In the interest of time and being prepared if necessary tomorrow, I attempted to capture some of what was said on the call so that we can use this publicly and with the Hill. I know that you are working on some of the additional details, Jennifer, and those will be helpful to weave into this, but I wanted to get this started in the meantime. Some of this is based on previously approved language. The new additions based on the call are in red. Could you route these to the right folks on your end? The goal is to get this cleared ASAP tomorrow morning. Attached is the full security packet, that includes the previous statements and background that we have used (for reference).

Please let me know if there's anything else I can do to help move this through the process-- figured it was easiest to just send to the two of you.

Thanks very much,
Jen

**(b)(5)**

**(b)(5)**

**(b)(5)**

(b)(5)

Not for Distribution/ Pre-Decisional/ Draft/ Deliberative

# SECURITY STATEMENTS/ BACKGROUND

**Contents:**



**(b)(5)**

(b)(5)

**KEY POINTS- SECURITY AND THE HUB:**

**Statement from CMS spokesperson:** "The privacy and security of consumers' personal information are 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. The components of the HealthCare.gov website that are operational have been determined to be compliant with the Federal Information Security Management Act (FISMA), based on standards promulgated by the National Institutes of Standards and Technology (NIST)."

**From CMS Data Hub Fact Sheet:**
CMS developed the Marketplace systems consistent with federal statutes, guidelines, and industry standards that help ensure the security, privacy, and integrity of the systems and the data that flow through them. All of CMS's 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 standards promulgated by HHS, the Office of Management and Budget, the Department of Homeland Security, and the National Institute of Standards and Technology.

CMS has designed the Hub, a routing tool that helps Marketplaces provide accurate and timely eligibility determinations. **The Hub will verify data against information contained in already existing, secure and trusted Federal and state databases. CMS will have security and privacy agreements with all Federal agencies and states connecting to the Hub.**

**The Hub and its associated systems have several layers of protection in place to mitigate information security risk.** For example, Marketplace systems will employ a continuous monitoring model that will utilize sensors and active event monitoring to quickly identify and take action against irregular behavior and unauthorized system changes that could indicate a potential incident.

The privacy and security of consumer data is a top priority for HHS and CMS. **The Hub and its associated systems have been built with state-of-the art business processes based on federal and industry standards. CMS has developed an extremely strong enterprise information security program to protect consumer information in a secure and efficient manner during open enrollment and beyond.**

**The Hub was specifically designed to minimize security risk, by developing a system that does not retain or store Personally Identifiable Information.**

**Fact sheet on the datahub, how it works, and its security:**
http://www.cms.gov/Newsroom/MediaReleaseDatabase/Fact-Sheets/2013-Fact-Sheets-Items/2013-09-11.html

**ADDITIONAL BACKGROUND: PRIVACY AND PII AND THE HUB:**

**9/11 – House Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies Holds Hearing on the Health Exchange Data Hub**
KAY DALY, ASSISTANT INSPECTOR GENERAL FOR AUDIT SERVICES, HEALTH AND HUMAN SERVICES DEPARTMENT

DALY: **It's important to note that the Hub does not store data, rather, it simply acts as a conduit for the exchanges to access data from where they are stored**
[…]

**How does the Data transfer work between agencies? Is it secure?**

**Henry Chao 11/19 House E&C hearing:**
CHAO: "The data services hub goes out and for a requester of that data, a valid requester, it reaves (ph) the data where the sources transfers it back to the requester in a secure fashion, does not remember the contents of that data and facilitates that without moving massive, you know, millions of records of data all at once, all the time every day. It only transfers enough data to get the job done."

**(b)(5)**

(b)(5)

(b)(5)

**Michael Finkel, Executive VP of Program Delivery, QSSI (from 9/10 House E&C Hearing with Contractors):**

FINKEL: We expect the Data Services Hub will be ready for CMS to operate as planned on October 1st.
[…]
FINKEL: We have completed software coding for the Data Services Hub for all functionality required for October 1st. We are continuing performance and integration testing.
[…]
FINKEL: CMS and its information security contractors will continually monitor the Data Services Hub. Government regulations require CMS to follow National Institute of Standards and Technology's security guidelines applicable to the Data Services Hub. The design and development of the Data Services Hub complies with these standards. **Additionally, the Data Services Hub has recently undergone an**

**independent security risk assessment by CMS's security assessment contractor, the Mitre Corporation. Our understanding is that that assessment did not identify any issues that would prevent CMS from launching the Data Services Hub on October 1st.** Once in production, CMS will enforce additional security controls to protect systems including controlling access and changes to the system. The Data Services Hub will continually be monitored by CMS and its information security contractors.

**Will there be a full SCA?**

OLSON: When can be, sir, that a full SCA will be conducted, system-wide?

CHAO: When the last pieces of the system are completely built, which is not **-- I don't want people to think that there hasn't been a full SCA. Full SCA has been conducted on the pieces that were needed for October 1st for eligibility enrolment. We have yet -- we still have to build the financial management aspects of the system which includes our accounting system and payment system and reconciliation system. Those will also have security testing involve as well.**

**SCAs based on Risk Mitigation (from 11/19 House E&C hearing):**

SCHAKOWSKY: So Mr. Chao, I want to walk through some of these keys security assessments to determine whether the high risks that MITRE identified we have in fact been addressed.
In January and February of 2013, MITRE of performed a security control assessment of EIDM (ph), the account creation function and healthcare.gov. According to the final report, MITRE identified several high risk findings. **So Mr. Chao, were these high risks findings resolved and mitigated before the October 1st start of open enrollment in the federal market place.**

CHAO: Yes, they were.

SCHAKOWSKY: And, the fact is that they were noted in the -- the backpack (ph) is noted in the MITRE report. **OK, so MITRE also performed the security control assessment of the data services hub in August, 2013. And again -- and again, identified several high risk findings. We're these findings result and also mitigated before the actual for first launch.**

CHAO: Yes, and the hub received an authority to operate in August.

SCHAKOWSKY: Yes and the fact is that was -- and that fact was noted in the report. **I also want to discuss the security control assessment that MITRE performed over August and September, 2013 for the heath insurance exchange. Mr. Chao, we're all high risks identified in this assessment mitigated before October 1st?**

CHAO: Yes.

SCHAKOWSKY: **Thank you and what your answers confirm is that a system worked, neither identified potentially high risk -- high security risk. And CMS made sure that they we're mitigated before they would become major problem. The MITRE reports do not show a flood system, they show that CMS conducted security control assessment to identify problems. And then fix those problems and I hope that my Republican collegues will keep these findings in mind when they took about the security of**

**healthcare.gov. We don't want to alarm the public about security risk and have a ready been addressed by CMS and in its contactors. It just seems to me that identifying risks that we're named. It's important also to note that they were all fixed before the launch on October 1st.** And I thank you very much for your testimony, I yield back.

**What was MITRE's roll in the SCA and ATO?**

**Testimony of Jason Providakes, MITRE, from 11/19 House E&C hearing:**
"As part of its efforts to establish healthcare.gov, CMS asked MITRE to conduct security assessments on parts of the site. And I appreciate this opportunity to clarify what our role was in assisting CMS on healthcare.gov. We provide CMS with information security support and guidance under two contracts, the Office of Information Systems and Enterprise Information Systems Group. Pursuing to task issued under those contracts, MITRE performed a total of 18 Security Control Assessments, or SCAs, for components across a range of CMS enterprise systems. Most of these were performed on supporting infrastructure and development components. Six of the SCAs were directly related to healthcare.gov and were performed between September 2012 and September of 2013.

MITRE is not in charge of security for healthcare.gov. We were not asked, nor did we perform end to end security testing. We have no view on the overall safety or security status of healthcare.gov.

MITRE did not and does not recommend approval or disapproval of an Authority to Operate. Deciding whether and when to grant an ATO is inherently a governmental function that derives from the government's assessment of overall risk posture. In this case, the government made its ATO decisions based on a large set of inputs and factors, among which were six SCAs performed by MITRE. We do not have visibility into the many other factors that went into the government's ATO decision. CMS did not advise MITRE whether or when ATOs were granted for the marketplace components being tested. In this case, the government made its ATO decisions based on a large set of data."

**(b)(5)**

(b)(5)

**What is CMS doing now to follow up on the risk mitigation strategies regarding ongoing security?**

**Henry Chao 11/19 House E&C hearing:**

CHAO: "On a daily basis, we run antivirus scans every three minutes. Now we run scans every three minutes. Data full monitoring is a continuous effort. Direct protection analysis against known bad IPs or hackers, I've mentioned that in the opening remarks, that it's continuous. On a weekly basis, we monitor operating system compliance, infrastructure system compliance, we conduct penetration testing authenticated and non-authenticated by marketplace security teams. We have a 24 by seven security operations team. We conduct additional penetration testing, authenticated and non-authenticated by another group of security professionals in CMS that report under our chief information security officer. We also conduct application software assurance testing which is occurring biweekly. And on a monthly basis, we produce a plan of actions and milestones that keeps track and reports on any discovered weaknesses during all this monitoring."

**WHAT IS THE PROCESS FOR REPORTING SECURITY INCIDENTS RE: Healthcare.gov?**

**HHS Spokesperson statement (11/19/13):**
The Department of Health and Human Services (HHS) continuously monitors all of our systems. Proactively identifying and addressing incidents is a regular part of that process. Incidents are any events that indicate that data or systems might have been compromised. To date, there is no indication that there has been a compromise of the Healthcare.gov system by an outside actor. And to date, we have handled a routine volume of incidents relating to HealthCare.gov.

We cannot provide a total number of incidents because, by their nature, our security assessments are a snapshot in time and our situational awareness of all our systems changes daily. To protect security, we do not get into details on the status of ongoing investigations.

(b)(5)

(b)(5)

**DISTINCTION BETWEEN SEPT 3 and SEPT 27 MEMOS**

**Description of Sept 3 and Sept 27 ATO Memos- Henry Chao testimony**

CMS Statement:

"The Sept 3 Authority to Operate memo is for two parts of HealthCare.gov, the Qualified Health Plans and Dental modules, and do not contain or use consumers' personal information-- they are the back-end systems tools that CMS uses to communicate plan certification information to the FFM. In addition, consumers do not use these tools. CMS acted on each of the two high findings in the Sept 3 memo by putting in place safeguards to mitigate risks."

(b)(5)

**STATEMENT ON CMS CONTRACTORS AND SECURITY**

**CMS Statement on Background- security and contractors (11/20/13):**

- The CMS contract for conducting Security Control Assessments will be at the end of its contract term in early 2014. This contract provides Security Controls Assessment for all CMS IT systems.

- Under federal contracting rules, CMS opened a competitive bid process to procure a new contract for these services. The Mitre contract was awarded in July 2009 and will expire at the end of January 2014. Mitre did not submit a bid for this new Request for Proposals.

- CMS awarded a new multi-year security testing contract in July 2013 to Blue Canopy. In September 2013, Blue Canopy supported testing of the FFM system and they will be the lead security testing contractor for the next FFM security assessment in December. Mitre will support the December assessment as their contract comes to a close. It's important to remember that security testing is an ongoing process which CMS must conduct on a regular basis following comprehensive NIST requirements.

- CMS has operational security protections in place including safeguards against distributed denial of service attacks. We also have in place weekly penetration testing, which is much more frequent than the yearly standard required by NIST.

- Creative Computing Solutions and their subcontractor, Foreground Security provide security monitoring services for HealthCare.gov. Booz Allen Hamilton has also provided support for software assurance activities, and SphereCom has supported security activities associated with the state-based marketplaces, State partnership model, and the Federally Facilitated Marketplace states.

**Additional Background:**

- The HealthCare.gov website has been determined to be compliant with the Federal Information Security Management Act (FISMA), based on standards promulgated by the National Institutes of Standards and Technology (NIST).

- Mitre conducted the Security Control Assessment (SCA) for the Data Services Hub and the Federally Facilitated Marketplace (FFM). The initial assessment of the enrollment function of the FFM was conducted during the last two weeks of August, and an initial draft report was issued by Mitre on August 30. The final assessment report by Mitre was issued on October.

- CMS leadership authorized operation of the FFM application on September 27. This authorization is limited to six months and prescribes a number of strategies to mitigate risks such as enhancing continuous monitoring and testing activities, and a requirement to perform a comprehensive 3rd party test in a single test environment before the end of the calendar year.

# Additional Background Points, as needed

**FISMA authority: How does this work?**

- The six-month authorization to operate represents a determination that the Federally Facilitated Marketplace (FFM) application is FISMA-compliant.
- All authorities to operate (ATOs) are required to have a termination date under FISMA guidance. There is currently a six-month authorization to operate in place for the FFM application. Security testing is happening on an ongoing basis using industry best practices and, under the terms and conditions of the ATO, technical experts are undertaking a number of strategies to mitigate risks. The six-month authorization to operate represents a determination that the FFM application is FISMA-compliant.
- CMS leadership issued an authorization to operate the FFM application on September 27, consistent with relevant security standards. This authorization is limited to six months and is conditioned on a number of strategies to mitigate risks outlined in the ATO, including regular testing.
- When a major change is made to a system, it must go through security testing again to ensure the major change has not compromised the security of the system, after which a new ATO is issued.
- The six-month authorization to operate is consistent with OMB guidance, which can be found below[i] and here: http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf.

**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 household member's behalf, individuals filing an application online may submit information about those household members, which is then subject to verification. The FFM 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 FFM does not show information about 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 and SSA determined that this use of information for verification purposes was a "routine use" under the Privacy Act.
- Under the Privacy Act, agencies with the necessary authority can 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 FFM constitutes a routine use. This is consistent with many other previously established routine uses under which information is provided for purposes of eligibility determinations in health maintenance or other government benefit programs, such as Medicaid, Social Security, and LIHEAP.

[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.[69]

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.[70] 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**: 10/8/2013 6:11:36 PM

**To**: Charest, Kevin (OS/ASA/OCIO/OIS) NotResp

**CC**: Schankweiler, Thomas W. (CMS/OIS) NotResp NotResp Mellor, Michael (CMS/OIS) NotResp NotResp

**Subject**: RE: Update request

**Attachments**: ffe_fortify_scan_breakout.jpg; Security Bug - report form

Kevin,

From the CISO's perspective, the following update is provided on the monitoring that is being conducted by EISG:

AppScan:

- Previously performed scans on 4 QHPs 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 CIISG 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 EIDM servers located at the Baltimore Data Center 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 Terremark/CIISG
- Internal testing – Testing of the internal devices at Terremark would require a VPN connection from the XOC or utilize the Management Band (would require opening firewalls). Given that testing of internal devices is currently being done by another component (the XOC, Foreground), I see little benefit from this line of testing from us.
    - This is still accurate at this time – if CIISG does transition to an alternate EIDM 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 XOC Security Team, as well as reviewing tickets ad-hoc in CALT as time permits.

nCircle/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.

RedSeal:

- Working on provisioning direct, read-only, access for XOC Security Team.
- Working on loading a new set of data from Terremark environment this week to perform updated reporting and analysis – Terremark 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 CCSI on the aggregator.
- Software Code is developed and comment on using the HP Fortify application tool (see attached sample). The developers have direct access to Fortify and they check in-and check out their code. The XOC Security Team actively reviews the code and also provides comments back to CGI. 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 CGI, QSSI, OC, EIDM 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. (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 security log aggregator?

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
HSDN: Kevin.Charest@dhs.sgov.gov

Ofc. 202-690-5548; Mobile 202-308-7565

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

**This space intentionally left blank.**

| Version | State |
| --- | --- |
| FFM_base | |
| base_6.2 | Last analysis results on 09/11/2013 2:43:49 AM |
| base_7.0 | Last analysis results on 10/07/2013 10:13:27 PM |
| FFM_base-trunk-mgmt-rest | |
| base-trunk-mgmt-rest_6.2 | Last analysis results on 09/11/2013 2:56:48 AM |
| base-trunk-mgmt-rest_7.0 | Last analysis results on 10/07/2013 10:26:30 PM |
| FFM_base-trunk-mgmt-ui | |
| base-trunk-mgmt-ui_6.2 | Last analysis results on 09/11/2013 3:07:19 AM |
| base-trunk-mgmt-ui_7.0 | Last analysis results on 10/07/2013 10:31:28 PM |
| FFM_common-eligibility-prime | |
| common-eligibility-prime_6.1 | Last analysis results on 09/11/2013 3:01:18 AM |

Message

**From:** Fryer, Teresa M. (CMS/OIS) NotResp NotResp
**Sent:** 12/20/2013 5:06:21 AM
**To:** Schankweiler, Thomas W. (CMS/OIS) NotResp NotResp Linares, George E. (CMS/OIS) NotResp NotResp
**CC:** Marantan, James (CMS/OIS) NotResp
**Subject:** FW: HC.GOV Update 12/20/1
**Attachments:** Healthcare.gov telecon read ahead.docx

**Importance:** High

Tom,

You need to be at this meeting looking at the attached agenda. James will be in attendance, however, these questions need to be answered by the Marketplace Security team.

Teresa Fryer, CISSP, HCISPP, CIPP/G
Chief Information Security Officer and
Director, Enterprise Information Security Group (EISG)
Centers for Medicare & Medicaid Services
Office of Information Services (OIS)
7500 Security Blvd, N1-26-18
Baltimore, MD 21244
410-786-2614 (W)
(b)(6) (C)
teresa.fryer@cms.hhs.gov

This space intentionally left blank.

---

**From:** Banghart, John [John_F_Banghart@nss.eop.gov]
**Sent:** Thursday, December 19, 2013 1:04 PM
**To:** Schlosser, Lisa; Penny, Erica (OS/ASA/OCIO); Ozment, Andy
**Cc:** Rudolph, Trevor; Charest, Kevin (OS/ASA/OCIO); Baitman, Frank (OS/ASA/OCIO); Nelson, David J. (CMS/OEM); Fryer, Teresa M. (CMS/OIS)
**Subject:** RE: HC.GOV Update 12/20/13

All,

Here is the read-ahead for tomorrow's teleconference that includes specific topic areas we would like to discuss. We expect HHS and CMS to have the necessary leadership and technical staff present on the call to address our concerns.

Please direct any questions or comments to me.

--
John Banghart
Director for Federal Agency Cybersecurity

National Security Staff, The White House
JBanghart@nss.eop.gov
(202) 456-9612

**From:** Schlosser, Lisa
**Sent:** Thursday, December 19, 2013 12:35 PM
**To:** Penny, Erica (OS/ASA/OCIO)
**Cc:** Rudolph, Trevor; Banghart, John
**Subject:** RE: HC.GOV Update 12/20/13

The NSS/OMB team is finalizing and will send shortly.

Thank you

**From:** Penny, Erica (OS/ASA/OCIO) [mailto:Erica.Penny@hhs.gov]
**Sent:** Thursday, December 19, 2013 12:18 PM
**To:** Schlosser, Lisa
**Subject:** HC.GOV Update 12/20/13

Good afternoon Ms. Schlosser,

Could you please provide me with a copy of the agenda for this call for Mr. Frank Baitman?

Thanks,
Erica Penny
Administrative Assistant
Office of the Chief Information Officer
Department of Health and Human Services
200 Independence Avenue, SW
Room 336E.3
Washington, DC 20201
(202) 205-4825
erica.penny@hhs.gov

Message

**From:** Schankweiler, Thomas W. (CMS/OIS NotResp
NotResp
on behalf of Schankweiler, Thomas W. (CMS/OIS)
**Sent:** 12/4/2013 2:59:41 AM
**To:** Peterson, Jason R. (CMS/CTR) NotResp
NotResp
**Subject:** FW: Security Items that Need Attention
**Attachments:** NotResp Ticket Status Update Requested by CMS 120313.docx

FYI

**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); Couts, 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:** FFM Security Defects
**Subject:** RE: Security Items that Need Attention

Please find attached a detailed update of the NotResp 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



**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 NotResp umbers 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

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); Couts, 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); Couts, 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.Couts1; 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:** Couts, 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 NotResp 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 NotResp
   - 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 Couts**
Centers for Medicare & Medicaid Services
Office of Information Services
301-492-5139 (office) | (b)(6) (mobile) | 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:** Couts, 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 DocumentFromECM?fileIdentifier=

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 DocumentFromECM?fileIdentifier=

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 DocumentFromECM?fileIdentifier=

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 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 DocumentFromECM?fileIdentifier=

Is NotResp 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)
(b)(6) (Mobile)
Adam.Willard@cms.hhs.gov

**CMS XOC Security Team**
Consumer Information & Insurance Systems Group (CIISG)
Centers for Medicare & Medicaid Services (CMS)
703-594-4961/703-910-3993
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 DocumentFromECM?fileIdentifier=

Hi Adam,

The eligibility notices are stored in NotResp 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 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 DocumentFromECM?fileIdentifier=
**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 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 XOC Security Team**
Consumer Information & Insurance Systems Group (CIISG)
Centers for Medicare & Medicaid Services (CMS)
703-594-4961/703-910-3993
ciisg-soc@cms.hhs.gov

# Status of FFM NotResp Tickets Created November 25, 2013

As of December 3, 2013

Many NotResp tickets were created on November 25, 2013. The vast majority were created upon CGI's request for system-related open security assessment findings (tracked in CFACTS as Plans of Action and Milestones [POA&Ms]). Using NotResp for the POA&Ms is necessary for them to be prioritized and worked on.

| NotResp Ticket # from Todd Couts | CGI IQ Suite ID | Defect or POA&M | Status | Comments |
|---|---|---|---|---|
| INC000002614246 | 8595 | Defect | Fixed in production on 11/21 | (b)(5) |
| INC000002614253 | 8596 | Defect | Open - Under Analysis | |
| INC000002614255 | 8597 | Defect | Open - Under Analysis | |
| INC000002614297 | 8599 | Defect | Open - Assigned to Resolution team | |
| INC000002614299 | 8674 | POA&M - Weakness #1 in CFACTS | Open - Reclassified from High to Moderate | |

# Status of FFM NotResp Tickets Created November 25, 2013

As of December 3, 2013

| NotResp Ticket # from Todd Couts | CGI IQ Suite ID | Defect or POA&M | Status | Comments |
|---|---|---|---|---|
| INC000002614303 | 8601 | POA&M - Weakness #6 in CFACTS | Open - Ready to be retested and recommended for closure | (b)(5) |
| INC000002614304 | 8677 | POA&M - Weakness #8 in CFACTS | Open | |
| INC000002614305 | 8657 | POA&M - Weakness #10 in CFACTS | Open | |
| INC000002614307 | 8656 | POA&M - Weakness #12 in CFACTS | Open | |
| INC000002614309 | 8654 | POA&M - Weakness #14 in CFACTS | Open | |
| INC000002614310 | 8653 | POA&M - Weakness #10 in CFACTS | Open | |
| INC000002614311 | 8652 | POA&M - Weakness #15 in CFACTS | Open | |
| INC000002614313 | 8678 | POA&M - Weakness #16 in CFACTS | Open | |
| INC000002614316 | 8679 | POA&M - Weakness #21 in CFACTS | Open | |

# Status of FFM NotResp Tickets Created November 25, 2013

As of December 3, 2013

| NotResp Ticket # from Todd Couts | CGI IQ Suite ID | Defect or POA&M | Status | Comments |
|---|---|---|---|---|
| INC000002614317 | 8687 | POA&M - Weakness #24 in CFACTS | Open - Finding was fixed with Finding #58 (Closed in the Findings spreadsheet managed by MITRE) in which JSESSIONIDs are terminated | (b)(5) |
| INC000002614318 | 8697 | POA&M - Weakness #26 in CFACTS | Open | |
| INC000002614319 | 8696 | POA&M - Weakness #27 in CFACTS | Open | |
| INC000002614320 | 8686 | POA&M - Weakness #29 in CFACTS | Open | |
| INC000002614321 | 8698 | POA&M - Weakness #33 in CFACTS | Open | |
| INC000002614322 | 8700 | POA&M - Weakness #36 in CFACTS | Open | |
| INC000002614323 | 8695 | POA&M - Weakness #37 in CFACTS | Open | |
| INC000002614324 | 8684 | POA&M - Weakness #44 in CFACTS | Open | |
| INC000002614325 | 8683 | POA&M - Weakness #45 in CFACTS | Open | |

# Status of FFM NotResp Tickets Created November 25, 2013

As of December 3, 2013

| NotResp Ticket # from Todd Couts | CGI IQ Suite ID | Defect or POA&M | Status | Comments |
|---|---|---|---|---|
| INC000002614326 | 8662 | POA&M - Weakness #46 in CFACTS | Open | (b)(5) |
| INC000002614328 | 8681 | POA&M - Weakness #48 in CFACTS | Open | |
| INC000002614329 | 8693 | POA&M - Weakness #49 in CFACTS | Open - Ready to be retested and recommended for closure | |
| INC000002614330 | 8701 | POA&M - Weakness #50 in CFACTS | Open - Ready to be retested and recommended for closure | |
| INC000002614331 | 8692 | POA&M - Weakness #51 in CFACTS | Open - Ready to be retested and recommended for closure | |
| INC000002614332 | 8690 | POA&M - Weakness #52 in CFACTS | Open | |
| INC000002614333 | 8698 | POA&M - Weakness #53 in CFACTS | Open | |
| INC000002614334 | 8675 | POA&M - Weakness #54 in CFACTS | Open - Ready to be retested and recommended for closure | |
| INC000002614335 | 8673 | POA&M - Weakness #55 in CFACTS | Open - Ready to be retested and recommended for closure | |
| INC000002614336 | 8685 | POA&M - Weakness #56 in CFACTS | Open | |
| INC000002614337 | 8680 | POA&M - Weakness #57 in CFACTS | Open | |
| INC000002614338 | 8671 | POA&M - Weakness #58 in CFACTS | Open | |
| INC000002614339 | 8670 | POA&M - Weakness #59 in CFACTS | Open | |

# Status of FFM NotResp Tickets Created November 25, 2013

As of December 3, 2013

| NotResp Ticket # from Todd Couts | CGI IQ Suite ID | Defect or POA&M | Status | Comments |
|---|---|---|---|---|
| INC000002614340 | 8669 | POA&M - Weakness #60 in CFACTS | Open | (b)(5) |
| INC000002614341 | 8668 | POA&M - Weakness #61 in CFACTS | Open | |

| Remedy Ticket # not provided by Todd Couts | CGI IQ Suite ID | Defect or POA&M | Status | Comments |
|---|---|---|---|---|
| INC000002614257 | 8598 | Defect | Fixed in production in Release 7.0.1.21 | (b)(5) |
| INC000002614301 | 8676 | POA&M - Weakness #61 in CFACTS | Closed | |
| INC000002614302 | 8600 | POA&M - Weakness #3 in CFACTS | Open - Ready to be retested and recommended for closure in QHP PROD | |
| INC000002614327 | 8682 | POA&M - Weakness #59 in CFACTS | Open | |

Message

**From:** Schankweiler, Thomas W. (CMS/OIS) NotResp NotResp
on behalf of Schankweiler, Thomas W. (CMS/OIS)
**Sent:** 12/2/2013 4:11:54 PM
**To:** Boulanger, Jennifer L. (CMS) NotResp NotResp Fryer, Teresa M. (CMS/OIS) NotResp NotResp Linares, George E. (CMS/OIS) NotResp NotResp
**CC:** Nelson, David J. (CMS/OEM) NotResp NotResp Aronson, Lauren (CMS/OL) NotResp NotResp Clark, Apryl C. (CMS/OL) NotResp NotResp Unruh, Patti (CMS/OC) NotResp NotResp
**Subject:** RE: URGENT -- Need review and comments ASAP
**Attachments:** SecurityandPrivacy-12-1-13 tw (4).docx

All,

I have edited as requested. Track Changes were enabled.

Thanks,

Tom

**From:** Boulanger, Jennifer L. (CMS)
**Sent:** Sunday, December 01, 2013 11:16 PM
**To:** Fryer, Teresa M. (CMS/OIS); Schankweiler, Thomas W. (CMS/OIS); Linares, George E. (CMS/OIS)
**Cc:** Nelson, David J. (CMS/OEM); Aronson, Lauren (CMS/OL); Clark, Apryl C. (CMS/OL); Unruh, Patti (CMS/OC)
**Subject:** RE: URGENT -- Need review and comments ASAP
**Importance:** High

I just received the word version of what is below. It should be easier to edit. Please send all edits back to Patti, Apryl and me as soon as you can. If we need a call to discuss, let us know asap. Thank you all very much and I apologize for the incredibly short time frame.

**From:** Boulanger, Jennifer L. (CMS)
**Sent:** Sunday, December 01, 2013 10:53 PM
**To:** Fryer, Teresa M. (CMS/OIS); Schankweiler, Thomas W. (CMS/OIS); Linares, George E. (CMS/OIS)
**Cc:** Nelson, David J. (CMS/OEM); Aronson, Lauren (CMS/OL); Clark, Apryl C. (CMS/OL); Unruh, Patti (CMS/OC)
**Subject:** URGENT -- Need review and comments ASAP
**Importance:** High

All – ASPA is working on statements that can be used if reporters call about the Mitre documents that we anticipate will be released to the press. This is an internal document and cannot be forwarded outside CMS.

Please review the statements below and send Patti Unruh, Apryl Clark and me your comments, corrections, additions first thing in the morning. Tom, George or I will call first thing to catch you up on what is going on. I have added some comments/questions in the document below in blue brackets.

Thank you for your help,

Jennifer

**From:** Friedman, Jennifer (OS/ASPA)
**Sent:** Sunday, December 01, 2013 10:19 PM
**To:** Boulanger, Jennifer L. (CMS); Unruh, Patti (CMS/OC)
**Cc:** O'Connor, Jen (OS/OGC); Flamberg, Gemma (HHS/OGC); Blackwood, Kristine (HHS/ASL); Scott, Meghan (HHS/ASL)
**Subject:** For review- follow-up from call

Hi Jennifer and Patti,

Following up on our call re: security today, below are some draft statements and Q/A for CMS review and approval. In the interest of time and being prepared if necessary tomorrow, I attempted to capture some of what was said on the call so that we can use this publicly and with the Hill. I know that you are working on some of the additional details, Jennifer, and those will be helpful to weave into this, but I wanted to get this started in the meantime. Some of this is based on previously approved language. The new additions based on the call are in red. Could you route these to the right folks on your end? The goal is to get this cleared ASAP tomorrow morning. Attached is the full security packet, that includes the previous statements and background that we have used (for reference).

Please let me know if there's anything else I can do to help move this through the process-- figured it was easiest to just send to the two of you.

Thanks very much,
Jen

(b)(5)

(b)(5)

(b)(5)

(b)(5)

Message

**From:** Schankweiler, Thomas W. (CMS/OIS) NotResp NotResp
on behalf of Schankweiler, Thomas W. (CMS/OIS)
**Sent:** 12/27/2013 7:21:04 PM
**To:** 'Goodrich, Lynn F (CGI Federal)' [lynn.goodrich@cgifederal.com]
**CC:** Banks, Stacey (CMS/CTR) NotResp NotResp Warren, Kevin (CMS/OIS) (Kevin.Warren@cms.hhs.gov) NotResp NotResp
**Subject:** RE: Security Items that Need Attention
**Attachments:** NotResp Ticket Status Update Requested by CMS 122713.docx

Lynn,

I went through NotResp see attached update. and I see that the NotResp tickets are still open.

- For POAM # 6, 8, 24, 36, 44, 21, 37, 58. We will need to wait until the next SCA to close out these as they are related specifically to the QHP.
- I highlighted nine that are currently under review by MITRE DB auditor and with any luck they will close out soon.
- We will need to work with you to get the remainder closed out.

I believe there are some more in remedy that need to be added to this list, but I did the cross check only one way from the word document to NotResp have not done the reverse verification yet.

Tom

**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); Couts, 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:** FFM Security Defects
**Subject:** RE: Security Items that Need Attention

Please find attached a detailed update of the NotResp 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

**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 NotResp 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

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); Couts, 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); Couts, 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.Couts1; 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:** Couts, 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 NotResp ticket your authorization to act. I am only sending the NotResp 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 NotResp
   - 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 Couts**
Centers for Medicare & Medicaid Services
Office of Information Services
301-492-5139 (office) | (b)(6) mobile) | 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:** Couts, 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 DocumentFromECM?fileIdentifier=

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 DocumentFromECM?fileIdentifier=

Hi Tom,
We promoted the code fix into production. Apparently the security enforcement is turned off.

Th 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 DocumentFromECM?fileIdentifier=

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 AlFresco. We expec 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 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 DocumentFromECM?fileIdentifier=

Is NotResp 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)
(b)(6) (Mobile)
Adam.Willard@cms.hhs.gov

**CMS XOC Security Team**
Consumer Information & Insurance Systems Group (CIISG)
Centers for Medicare & Medicaid Services (CMS)
703-594-4961/703-910-3993
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 DocumentFromECM?fileIdentifier=

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 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 DocumentFromECM?fileIdentifier=
**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 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)
Adam.Willard@cms.hhs.gov

**CMS XOC Security Team**
Consumer Information & Insurance Systems Group (CIISG)
Centers for Medicare & Medicaid Services (CMS)
703-594-4961/703-910-3993
ciisg-soc@cms.hhs.gov

# Status of FFM NotResp Tickets Created November 25, 2013

As of December 3, 2013

Many NotResp tickets were created on November 25, 2013. The vast majority were created upon CGI's request for system-related open security assessment findings (tracked in CFACTS as Plans of Action and Milestones [POA&Ms]). Using NotResp for the POA&Ms is necessary for them to be prioritized and worked on.

| NotResp Ticket # from road Couts | CGI IQ Suite ID | Defect or POA&M | Status | Comments | 12/27 NotResp |
|---|---|---|---|---|---|
| INC000002614246 | 8595 | Defect | Fixed in production on 11/21 | (b)(5) | Still opened and assigned to Reed Erickson |
| INC000002614253 | 8596 | Defect | Open - Under Analysis | | Still opened and assigned to Reed Erickson |
| INC000002614255 | 8597 | Defect | Open - Under Analysis | | Still opened and assigned to Reed Erickson |
| INC000002614297 | 8599 | Defect | Open - Assigned to Resolution team | | Still opened and assigned to Reed Erickson |
| INC000002614299 | 8674 | POA&M - Weakness #1 in CFACTS | Open - Reclassified from High to Moderate | | Still opened and assigned to Reed Erickson |

# Status of FFM NotResp Tickets Created November 25, 2013

As of December 3, 2013

| NotResp Ticket # from Todd Couts | CGI IQ Suite ID | Defect or POA&M | Status | Comments | 12/27 NotResp |
|---|---|---|---|---|---|
| INC000002614303 | 8601 | POA&M - Weakness #6 in CFACTS | Open - Ready to be retested and recommended for closure | NotResp | Still opened and assigned to Reed Erickson |
| INC000002614304 | 8677 | POA&M - Weakness #8 in CFACTS | Open | | Still opened and assigned to Reed Erickson |
| INC000002614305 | 8657 | POA&M - Weakness #10 in CFACTS | Open | | Still opened and assigned to Dhaval Patel |
| INC000002614307 | 8656 | POA&M - Weakness #12 in CFACTS | Open | | Still opened and assigned to Dhaval Patel |
| INC000002614309 | 8654 | POA&M - Weakness #14 in CFACTS | Open | | Still opened and assigned to Dhaval Patel |
| INC000002614310 | 8653 | POA&M - Weakness #10 in CFACTS | Open | | Still opened and assigned to Dhaval Patel |

NotResp

## Status of FFM I Tickets Created November 25, 2013

As of December 3, 2013

| NotResp Ticket # from Todd Couts | CGI IQ Suite ID | Defect or POA&M | Status | Comments | 12/27 NotResp |
|---|---|---|---|---|---|
| INC000002614311 | 8652 | POA&M - Weakness #15 in CFACTS | Open | | Still opened and assigned to Dhaval Patel |
| INC000002614313 | 8678 | POA&M - Weakness #16 in CFACTS | Open | | Still opened and assigned to Robert Walter |
| INC000002614316 | 8679 | POA&M - Weakness #21 in CFACTS | Open | | Still opened and assigned to Robert Walter |
| INC000002614317 | 8687 | POA&M - Weakness #24 in CFACTS | Open - Finding was fixed with Finding #58 (Closed in the Findings spreadsheet managed by MITRE) in which JSESSIONIDs are terminated | (b)(5) | Still opened and assigned to Dhaval Patel |
| INC000002614318 | 8697 | POA&M - Weakness #26 in CFACTS | Open | | Still opened and assigned to Dhaval Patel |
| INC000002614319 | 8696 | POA&M - Weakness #27 in CFACTS | Open | | Still opened and assigned to Dhaval Patel |
| INC000002614320 | 8686 | POA&M - Weakness #29 in CFACTS | Open | | Still opened and assigned to Dhaval Patel |

# Status of FFM NotResp Tickets Created November 25, 2013

As of December 3, 2013

| NotResp Ticket # from Todd Couts | CGI IQ Suite ID | Defect or POA&M | Status | Comments | 12/27 NotResp |
|---|---|---|---|---|---|
| INC000002614321 | 8698 | POA&M - Weakness #33 in CFACTS | Open | (b)(5) | Still opened and assigned to Dhaval Patel |
| INC000002614322 | 8700 | POA&M - Weakness #36 in CFACTS | Open | | Still opened and assigned to Michael Haynes |
| INC000002614323 | 8695 | POA&M - Weakness #37 in CFACTS | Open | | Still opened and assigned to Dhaval Patel |
| INC000002614324 | 8684 | POA&M - Weakness #44 in CFACTS | Open | | Still opened and assigned to Dhaval Patel |
| INC000002614325 | 8683 | POA&M - Weakness #45 in CFACTS | Open | | Still opened and assigned to Dhaval Patel |
| INC000002614326 | 8662 | POA&M - Weakness #46 in CFACTS | Open | | Still opened and assigned to Reed Erickson |
| INC000002614328 | 8681 | POA&M - Weakness #48 in CFACTS | Open | | Still opened and assigned to Dhaval Patel |

# Status of FFM NotResp Tickets Created November 25, 2013

As of December 3, 2013

| NotResp Ticket # from Todd Couts | CGI IQ Suite ID | Defect or POA&M | Status | Comments | 12/27 NotResp |
|---|---|---|---|---|---|
| INC000002614329 | 8693 | POA&M - Weakness #49 in CFACTS | Open - Ready to be retested and recommended for closure | (b)(5) | Still opened and assigned to Dhaval Patel |
| INC000002614330 | 8701 | POA&M - Weakness #50 in CFACTS | Open - Ready to be retested and recommended for closure | | Still opened and assigned to Michael Haynes |
| INC000002614331 | 8692 | POA&M - Weakness #51 in CFACTS | Open - Ready to be retested and recommended for closure | | Still opened and assigned to Michael Haynes |
| INC000002614332 | 8690 | POA&M - Weakness #52 in CFACTS | Open | | Still opened and assigned to Michael Haynes |
| INC000002614333 | 8698 | POA&M - Weakness #53 in CFACTS | Open | | Still opened and assigned to Michael Haynes |
| INC000002614334 | 8675 | POA&M - Weakness #54 in CFACTS | Open - Ready to be retested and recommended for closure | | Still opened and assigned to Dhaval Patel |
| INC000002614335 | 8673 | POA&M - Weakness #55 in CFACTS | Open - Ready to be retested and recommended for closure | | Still opened and assigned to Dhaval Patel |
| INC000002614336 | 8685 | POA&M - Weakness #56 in CFACTS | Open | | Still opened and assigned to Michael Haynes |

# Status of FFM NotResp Tickets Created November 25, 2013

As of December 3, 2013

| NotResp Ticket # from Todd Couts | CGI IQ Suite ID | Defect or POA&M | Status | Comments | 12/27 NotResp |
|---|---|---|---|---|---|
| INC000002614337 | 8680 | POA&M - Weakness #57 in CFACTS | Open | (b)(5) | Still opened and assigned to Michael Haynes |
| INC000002614338 | 8671 | POA&M - Weakness #58 in CFACTS | Open | | Still opened and assigned to Dhaval Patel |
| INC000002614339 | 8670 | POA&M - Weakness #59 in CFACTS | Open | | Still opened and assigned to Dhaval Patel |
| INC000002614340 | 8669 | POA&M - Weakness #60 in CFACTS | Open | | Still opened and assigned to Dhaval Patel |
| INC000002614341 | 8668 | POA&M - Weakness #61 in CFACTS | Open | | Still opened and assigned to Dhaval Patel |

# Status of FFM NotResp Tickets Created November 25, 2013

As of December 3, 2013

| NotResp Ticket # not provided by Todd Couts | CGI IQ Suite ID | Defect or POA&M | Status | Comments | 12/27 NotResp |
|---|---|---|---|---|---|
| INC000002614257 | 8598 | Defect | Fixed in production in Release 7.0.1.21 | (b)(5) | Still opened and assigned to Reed Erickson |
| INC000002614301 | 8676 | POA&M - Weakness #61 in CFACTS | Closed | | Still opened and assigned to Reed Erickson |
| INC000002614302 | 8600 | POA&M - Weakness #3 in CFACTS | Open - Ready to be retested and recommended for closure in QHP PROD | | Still opened and assigned to Reed Erickson |
| INC000002614327 | 8682 | POA&M - Weakness #59 in CFACTS | Open | | Still opened and assigned to Dhaval Patel |

Message

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

on behalf of Schankweiler, Thomas W. (CMS/OIS)

**Sent:** 11/8/2013 5:05:19 PM

**To:** Chao, Henry (CMS/OIS) [ NotResp

**CC:** Outerbridge, Monique (CMS/OIS) [ NotResp NotResp Grothe, Kirk A. (CMS/OIS) NotResp NotResp

**BCC:** Warren, Kevin (CMS/OIS) (Kevin.Warren@cms.hhs.gov) NotResp NotResp Burke, Sheila M. (CMS/OIS) NotResp NotResp Lyles, Darrin V. (CMS/OIS) (Darrin.Lyles@cms.hhs.gov) NotResp

**Subject:** Security Testing for FFM - 2013 summary and evidence files

**Attachments:** FFM August 2013 SCA FINAL_Test_Plan-08 21 2013.pdf; FFM ATO_Sep_3_2013.pdf; FFM decision memo.pdf; HIX Dental FINAL SCA Report 07152013.pdf; HIX-A Final SCA Report 10112013.pdf; HIX-A-Blue_Canopy_Security_Control_Assessment_Test_Plan_20130917.pdf; HIX August 2013 SCA FINAL_Test_Plan-08 21 2013.pdf; HIX-A September 2013 SCA Final_Test_Plan-09 17 2013.pdf; HIX-A-Blue_Canopy_SCA_Report.pdf; HIX-A - Daily Briefing Agenda 2013 09 20.pdf

Henry,

This e-mail contains sensitive and confidential information. Please limit distribution, see disclaimer at bottom of message.

Contract information:

MITRE: SCA activities under Task Order No . HHSM-500-2009-00021U

Blue Canopy: SCA activities under Task Order No. HHSM500-2013-00054U

GTL: Jessica Hoffman

COR: Heidi Myers, and recently changed to Alex Coles

Per your request and our discussion I have annotated a timeline showing several key activities.

1) Delivery of Test Plans,
2) On Site testing dates,
3) Final SCA test reports,
4) Dates of ATO memos.

To support this summary a reference to each activity is listed which is directly related to an attached document as evidence.

May XX, 2013

(Security Test plan needed here) I have requested this from MITRE as I do not have a copy of it.

**June 3-7, 2013**

MITRE was on site, at the CGI facility.

Security Control testing for HIX QHP and Dental modules started on June 3rd and ran through June 7th

Ref: HIX Dental Final SCA Report 07152013.pdf

**July 15, 2013**
MITRE delivered a "Final" SCA report for HIX and QHP and Dental Module
Ref: HIX Dental Final SCA Report 07152013.pdf

**August 19-30, 2013**
MITRE was on-site at the CGI facility.
Security Control Testing for HIX started Aug 19th and ran through August 30th.
Ref: HIX August 2013 SCA Final Test Plan 08-21-2013.pdf

**August 21, 2013**
MITRE delivered a "final" Security Test Plan,
Health Information eXchange (HIX), Quality Health Plans (QHP), August 2013 Security Controls Assessment Test Plan
The plan was finalized after the start of the assessment as some details of the assessment were submitted just days before the test began.
Ref: HIX August 2013 SCA Final Test Plan 08-21-2013.pdf

**September 3, 2013**
The FFM ATO memo was signed by Tony Trenkle for the Federally Facilitated Marketplace (FFM) aka. HIX. The ATO was limited the authorization to the tested modules being QHP and Dental modules of FFM only.
Ref: FFM ATO Sep 3, 2013.pdf

**September 16-20, 2013**
MITRE and Blue Canopy on-site at the CGI facility.
Security Control Testing for HIX started Aug 16th and ran through August 20th.
Ref: HIX-A September 2013 SCA Final_Test_Plan-09172013.pdf

**September 17, 2013**
MITRE delivered a "Final" Continued Health Information eXchange (HIX), August 2013 Security Controls Assessment Test Plan
The plan was finalized after the start of the assessment as some details of the assessment were submitted just days before the test began.
Ref: HIX-A September 2013 SCA Final_Test_Plan-09172013.pdf

Blue Canopy delivered a "Final" Security Control Assessment Test plan
Ref: HIX-A Blue Canopy Security Control Assessment Test Plan 20130917.pdf

**September 20, 2013**
MITRE delivered a final out-brief and annotated all of the open findings in a separate spreadsheet. This briefing, report, and weakness spreadsheet were used as the basis for the development of the Sep 27 decision memo created by Teresa Fryer, CISO and Tony Trenkle, CIO.
Ref: HIX-A Daily Briefing Agenda 2013_09_20.pdf

**September 27, 2013**
A FFM Decision memo was signed by Marilyn Tavenner

The memo sites that CMS utilized independent and specialized contractors [*MITRE and Blue Canopy*] to conduct testing in September of the FFM Eligibility and Enrollment (E&E), Financial Management (FM) Modules
Ref: FFM decision memo.pdf

**October 11, 2013**
MITRE delivered a "Final" Security Control Assessment Report
This report refers to the September testing of E&E, FM, and PM modules and only contains MITRE's findings for the August and September 2013
assessments of the HIX application. Findings from Blue Canopy are reported separately.
Ref: HIX-A Final SCA Report 10112013.pdf

**October 15, 2013**
Blue Canopy delivered a "Draft" Security Control Assessment Report
Ref: HIX-A Blue Canopy SCA Report.pdf

*Future Plans:*

**Dec 6,**
Blue Canopy will deliver a Final SCA Test Plan, that contains the combined efforts expected for MITRE and Blue Canopy

**December 9-20, 2013**
MITRE and Blue Canopy will conduct a Comprehensive Security Control Assessment for the FFM.

**Late January 2014**
ATO letter from CIO expected

End of report:

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)

**This space intentionally left blank.**

# HIX-A Security Control Assessment
# Daily Briefing Agenda

**Date: Friday September 20, 2013**
**Time: 4:00 – 4:30pm**
**Bridge Number / Pass Code:** (b)(6)

(b)(6)

## Agenda

- Review of findings. Please refer to the spreadsheet "*HIX-A Assessment Findings 2013 09 20.xlsx*"
  - New
    - 1 Moderate (BC-8)
  - Totals:
    - Blue Canopy: 3 Moderates, 5 Lows
    - MITRE:

NotResp

## Discussion:

- Blue Canopy testing: (see *Blue Canopy Testing Responsibilities Page 3 sbelow*)
  - E&E: Direct Enrollment – 75% *Complete*
  - E&E: Call Center –70% *Complete* ( 5/7 modules )
  - PM: Plan Certification – *100% Complete*

- MITRE Testing (see *MITRE Testing Responsibilities Page 4 below*)
  - Viewed most of the functionally
    - Lite SCA testing occurred in the ProPrime environment starting Wednesday September 18, 2013 after 17:00.
    - No active vulnerability tests were performed that might bring down the environment per CMS direction.
      - Email address spoofing, Malicious file uploading ,Input validation, No Denial of Service attempts was not performed.
    - Confirmation of functionality was performed, which included minor input validation, and retesting of August 2013 SCA findings

- Testing Schedule going forward
  - Remote verification testing of HIGH finding, when available till 17:00 today
  - Call Center UI – will be tested next Friday September 27, 2013 by Blue Canopy
  - Notices and Mailing: will be tested next Friday September 27, 2013 by Blue Canopy

# Action Item Status – All action items are closed

## Meeting Schedule

| Completed | Day / Date | Time | Meeting |
|---|---|---|---|
| X | Mon 9/16 | 9:30 -10:00 | Kick off Meeting |
| X | | 10:00 - 11:00 | Application Walkthroughs<br>○ My Account<br>○ Individual account<br>○ Plan Ratification<br>○ Individual Application<br>○ Call Center |
| X | Tue 9/17 | - | Application Walkthroughs<br>○ Direction Enrollment<br>○ Plan Compare |
| X | | 4:00 – 4:30 | SCA Daily Outbrief |
| X | Wed 9/18 | 4:00 – 4:30 | SCA Daily Outbrief |
| X | Thu 9/19 | 4:00 – 4:30 | SCA Daily Outbrief |
| X | Fri 9/20 | 4:00 – 4:30 | **FINAL** SCA Outbrief |

## SCA Schedule

### Estimated Timeline for Assessment Actions and Milestones (from Test Plan)

| Action/Milestone | Description | Date(s) |
|---|---|---|
| Establish and test accounts | Set up and test all test accounts for the assessment | Monday September 16, 2013 |
| Finalize and deliver Final Test Plan | Update the final test plan to include all action items, decisions, interview schedules, and other information from the Draft Test Plan Discussion | Tuesday September 17, 2013 |
| Perform onsite assessment | Conduct technical testing and management and operations interviews based on the assessment's scope | September 16-19, 2013 |
| Conduct final out brief | Review and summarize security vulnerabilities from assessment | Friday September 20, 2013 |
| Last date to provide remediation evidence (if authorized by CMS Facilitator) | CMS Division of Information Security & Privacy Management strongly advices that the focus of remediation efforts be on addressing High risk findings, followed by Moderate risk findings. | Thursday September 19, 2013 @ 5pm, High Finding Friday September 20, 2013 |
| Remove security access | Remove security access established for MITRE test accounts | ~~Thursday September 19, 2013 @ 5pm~~ Friday September 20, 2013 |
| Deliver draft report to CMS | Put security vulnerabilities identified during the assessment into report format | Monday September 23, 2013 |
| Review draft report | Answer questions and provide clarification. Only security vulnerabilities reported during the assessment and included in the final out brief are included in the report | Friday September 27, 2013 |
| Deliver final report and data worksheet to CMS | Edit and clarify the draft report and generate a data worksheet | Friday October 4, 2013 |
| Deliver final book package to CMS | Produce and provide hardcopies of test scripts, test data, out briefs, the final report, and the data worksheet(s) with a CD containing this information to the CMS SCAs GTL | Friday October 11, 2013 |

# Testing Responsibilities

## Blue Canopy Testing

| Module | Capability | Status | Functionality | Status |
|---|---|---|---|---|
| E&E | Direct Enrollment | waiting | Issuer redirects consumer to FFM to complete application & determine eligibility | 9/19/2013 - In order to test the direct enrollment link testing, we will need to change environments or acquire separate certificates from Terremark. |
| | Direct Enrollment | completed | Issuer retrieves eligibility information on consumer's household from FFM | 9/19/2013 - Tested in "Test2" environment - COMPLETED |
| | Direct Enrollment | completed | Consumer submits enrollment transaction | 9/19/2013 - Tested in "Test2" environment - COMPLETED |
| | Direct Enrollment | completed | Consumer submits cancellation transaction | 9/19/2013 - Tested in "Test2" environment - COMPLETED |
| | Enrollment | | Initial Enrollment and Change Enrollment (Cancel / Terminate) [Tentative] | 9/19/2013 - Waiting on Mohan (CGI Federal) to be seen, will continue testing September 27, 2013 |
| | Enrollment | completed | Outbound 834s for Issuers (Initial / Change / Cancel / Terminate) | 9/19/2013 - COMPLETED |
| | Enrollment | | Process Inbound 834s from Issuers (Effectuate / Cancel / Terminate) | Waiting on Data, will test Friday September 27, 2013 |
| | Enrollment | completed | Transaction Logging (999, 834, Business Acknowledgement) | 9/19/2013 - COMPLETED |
| | Call Center | completed | FFM - Next Generation Desktop (NGD) Interfaces - Find Person & Find Authorized Representative Interfaces | 9/19/2013 - COMPLETED |
| | Call Center | completed | Find / retrieve application and application details | 9/19/2013 - COMPLETED |
| | Call Center | completed | Escalate issues to Eligibility Support Worker | 9/19/2013 - COMPLETED |
| | Call Center | completed | Retrieve activity log | 9/19/2013 - COMPLETED |
| | Call Center | completed | Unlock Account / Reset Forgotten Password | 9/19/2013 - COMPLETED |
| | Call Center | | CCRs use FFM for applications and plan shopping / selection | will test Friday September 27, 2013 |
| | Call Center | | Mailing Contractor Integrations (Notices themselves are displayed on Bulletin Board in My Account Message Center) | Waiting on Data, will test Friday September 27, 2013 |
| PM | Plan Certification | completed | Plan Certification | Reviewed findings with development team; Complete |
| | | | | |

# MITRE Testing

Lite SCA testing occurred in the ProPrime environment starting Wednesday September 18, 2013 after 17:00.
No active vulnerability tests were performed that might bring down the environment per CMS direction.
Email address spoofing, Malicious file uploading ,Input validation, No Denial of Service attempts was not performed.
Confirmation of functionality was performed, which included minor input validation, and retesting of August 2013 SCA findings

| Module | Capability | Functionality | Status |
|---|---|---|---|
| E&E | Create Account | My Account - Identity Proofing - Online & Account Creation with ability to view eligibility and enrollment status | ID Proofing via Online - tested - completd<br>ID Proofing via Document upload - process not fully tested due to confirmation not received<br>ID Proofing via Calling Experian could not be tested, functionality not available. |
| | Create Account | My Account - Message Center & Notices Displayed on Bulletin Board | |
| | Create Account | My Account - Eligibility Results & Appeals | |
| | Create Account | My Account - Terminate / Cancel Coverage | |
| | Complete Application | Eligibility Results | |
| | Complete Application | Household Contact | |
| | Complete Application | Income | |
| | Complete Application | Income Screener / Help Paying for Coverage | |
| | Complete Application | Insurance | |
| | Complete Application | Build Household, Personal Information & Household Summary - Individual | |
| | Complete Application | Build Household, Personal Information & Household Summary - Household limited to single tax household | |
| | Complete Application | Attestations | |
| | Complete Application | Enrollment Period / SEP Questions | |
| | Complete Application | Delayed Response | |
| | Complete Application | Special Circumstances | |

| | | | |
|---|---|---|---|
| | Complete Application | Assister Identification | |
| | Eligibility Determination | Complete eligibility / determine individual eligibility: Medicaid/CHIP based on MAGI | |
| | Eligibility Determination | Complete eligibility / determine individual eligibility: Medicaid based on non-MAGI factors | |
| | Eligibility Determination | Complete eligibility / determine individual eligibility: Advance Premium Tax Credits (APTC) | not tested, valid test data was not provided to completely see functionality of APTC |
| | Eligibility Determination | Complete eligibility / determine individual eligibility: Cost Sharing Reduction (CSR) | not tested, valid test data was not provided to completely see functionality of CSR |
| | Eligibility Determination | Verification- ESC MEC | |
| | Eligibility Determination | Verification - Non ESC MEC | |
| | Eligibility Determination | Verification - Annual Income | |
| | Eligibility Determination | Verification - Citizenship | |
| | Eligibility Determination | Verification - Lawful Presence | |
| | Plan Compare | Payment redirect | |

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

CENTERS for MEDICARE & MEDICAID SERVICES

***CENTERS FOR MEDICARE & MEDICAID SERVICES***

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

# *Federally Facilitated Marketplace (FFM) [HIX-A] Security Control Assessment (SCA) Report*

***Blue Canopy***
***Draft Report***

**September 30, 2013**

# Table of Contents



(b)(5)

NotResp

# List of Tables



# List of Figures

# 1. EXECUTIVE SUMMARY

The Centers for Medicare and Medicaid Services (CMS) of the United States Department of Health and Human Services (HHS) engaged MITRE and Blue Canopy to perform a joint onsite comprehensive application security control assessment (SCA) of the Federally Facilitated Marketplace (FFM, also referenced as HIX-A) major application as part of the CMS Certification and Accreditation (C&A) Program. Blue Canopy conducted (1) a review to ensure that the application complied with CMS security instructions, (2) a configuration review to determine if security controls were implemented correctly, (3) interviews, and (4) documentation reviews to determine if security controls were implemented correctly.

## 1.1 Federally Facilitated Marketplace Background

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

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

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

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

CCIIO will manage the Marketplace program and enable collaboration through 1) the use of a cloud-based infrastructure that is Federal Information Security Management Act (FISMA) compliant and can be dynamically scaled as needed, and 2) a secured cloud-based ALM that

functions as a component of a Platform as a Service (PaaS). These tools are essential in supporting the following capabilities:

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

## 1.2 Assessment Scope

To determine the potential security risks to CMS, Blue Canopy was tasked with providing a comprehensive scope application SCA of the Federally Facilitated Marketplace major application located at the CGI Federal contractor facilitate, 593 Herndon Parkway, Herndon, Virginia. The application was assessed from September 16-19. In accordance with the Security Control Assessment Test Plan, Blue Canopy performed the following activities during the independent assessment:

- Interviewed selected personnel
- Performed application security testing

As part of this assessment, Blue Canopy teamed with MITRE to complete the application testing for this assessment. MITRE was responsible for all controls testing outside of the application testing itself. The application module testing scope was assigned by CMS and supplied to the testing teams upon arrival onsite for the assessment. The identified scope for Blue Canopy was as follows:

| Capability | Functionality | UI or Backend Process |
|---|---|---|
| Direct Enrollment | Issuer redirects consumer to FFM to complete application & determine eligibility | UI |
| Direct Enrollment | Issuer retrieves eligibility information on consumer's household from FFM | Backend |
| Direct Enrollment | Consumer submits enrollment transaction | Backend |
| Direct Enrollment | Consumer submits cancellation transaction | Backend |

| | | |
|---|---|---|
| Enrollment | Initial Enrollment and Change Enrollment (Cancel / Terminate) | Backend |
| Enrollment | Outbound 834s for Issuers (Initial / Change / Cancel / Terminate) | Backend |
| Enrollment | Process Inbound 834s from Issuers (Effectuate / Cancel / Terminate) | Backend |
| Enrollment | Transaction Logging (999, 834, Business Acknowledgement) | Backend |
| Call Center | FFM - Next Generation Desktop (NGD) Interfaces - Find Person & Find Authorized Representative Interfaces | Backend |
| Call Center | Find / retrieve application and application details | Backend |
| Call Center | Escalate issues to Eligibility Support Worker | Backend |
| Call Center | Retrieve activity log | Backend |
| Call Center | Unlock Account / Reset Forgotten Password | Backend |
| Call Center | CCRs use FFM for applications and plan shopping / selection | UI |
| Plan Certification | Plan Certification | UI |
| Notices and Mailing | Mailing Contractor Integration | UI |

Testing environment varied during the week between Prod Prime, Imp1a, and Test2, with a significant enough outage around all environments on Monday that no testing took place. The result of the testing for each of the above capabilities:

Direct Enrollment – Heavy backend NotResp testing of the interfaces. The minor web interface was not accessible for testing.

Enrollment – Outbound NotResp message functionality was validated. For the incoming NotResp messages managing the inbound 834 messages, the operating system functionality/permissions were successfully reviewed in order to validate that the file queue was secure. Validation of the parsing of the 834 messages by the Enrollment module was also conducted.

Call Center – All call center backend API interfaces were heavily tested with NotResp messages attacks, and no issues were identified. A call center UI was being deployed and was only available for limited security testing at the time that the assessment concluded.

Plan Certification – UI testing was completed with minimal findings.

Notices and Mailing – This was a minor UI component of static plan page displays and received some security testing

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

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

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

## 1.3 Summary of Findings

Of the 9 findings discovered by Blue Canopy in the system, none were considered High risks, 4 Moderate risks, and 5 Low risks. The risks found during the assessment are broken down as shown on the graph in Figure 1.

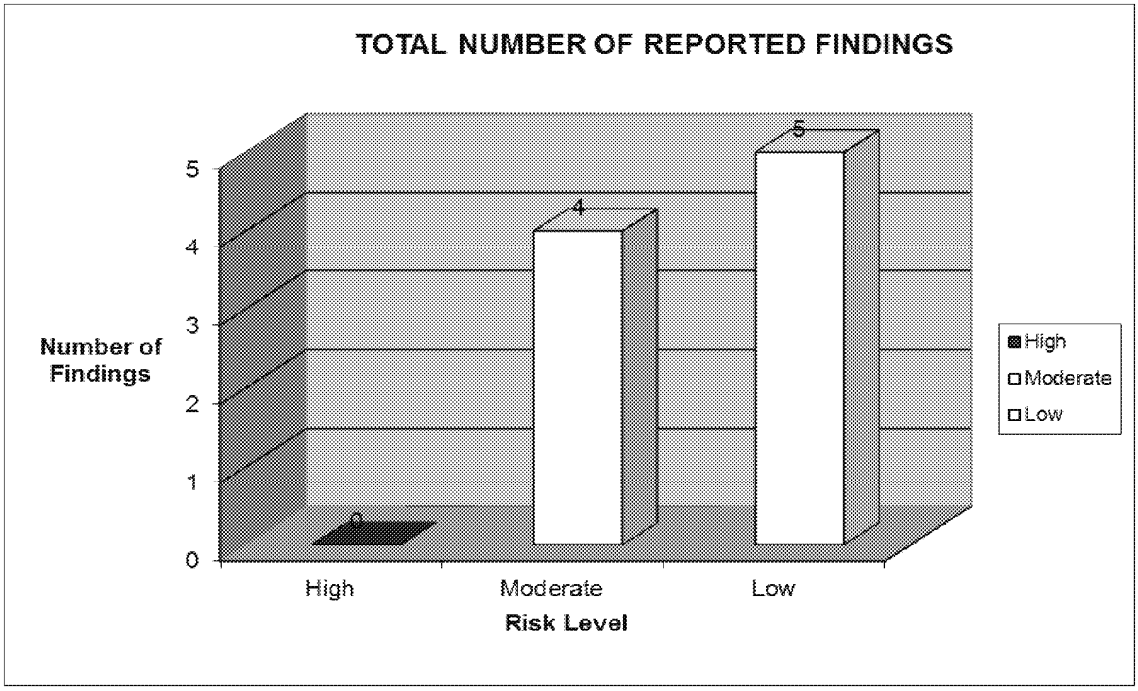



**Figure 1. Reported Findings by Risk Level**

No findings were able to be closed during the assessment. As a result, of the 9 initial findings discovered in the system, the 4 Moderate risk findings and 5 Low risk findings remain open. The risks remaining during the assessment are broken down as shown on the graph in Figure 2.

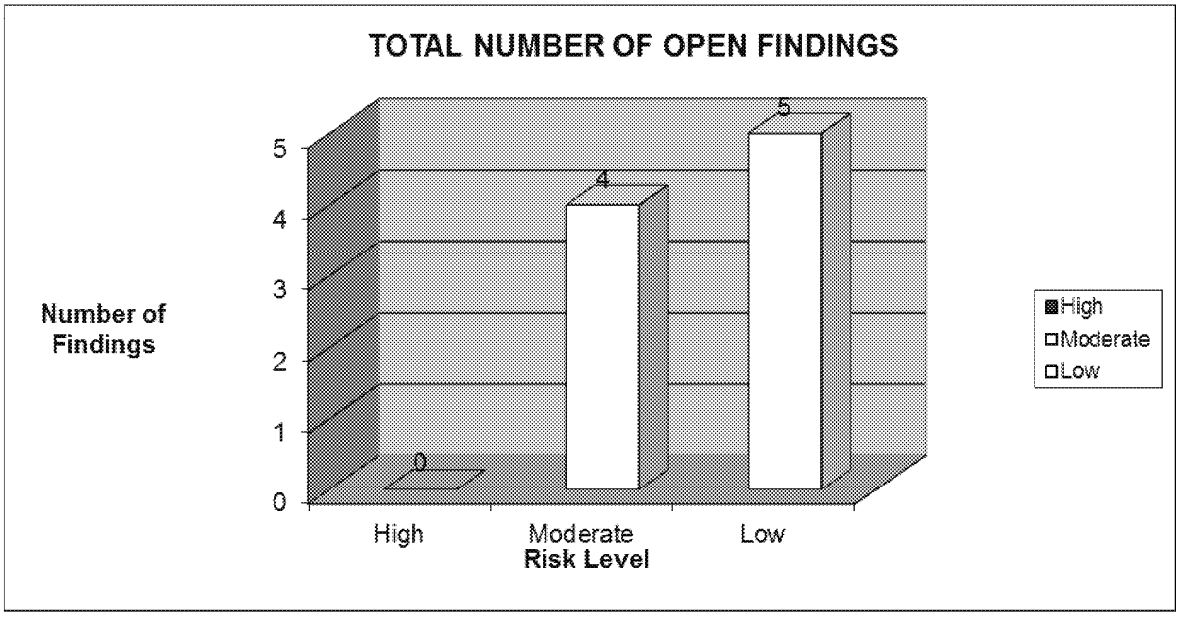



**Figure 2. Open Findings by Risk Level**

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

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

## 1.4 Summary of Recommendations

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

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

**Publically Accessible Data:** Using NotResp data was accessed that should not be publically accessible. We recommend considering the potential security risks from divulging this data and implementing appropriate controls.

# 2. INTRODUCTION

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

The Federal Information Security Management Act (FISMA) of 2002 passed as TITLE X of The Homeland Security Act and signed into law on November 27, 2002, and the TITLE III of the E-Government Act of 2002 signed into law on December 17, 2002, reinforces CMS efforts to protect the business processes supported by information technology (IT) platforms. The purpose of the Security Control Assessment is to adhere to the *CMS Information Security (IS) Assessment Procedure Version 2.01*[1] that establishes a uniform approach for the conduct of information security (IS) testing of the CMS Information Systems for Major Applications (MA) and their underlying component application systems.

Blue Canopy was tasked with conducting a security control assessment (SCA) of the Federally Facilitated Marketplace (FFM, also known as HIX) to determine the overall risk the system presents to CMS. The onsite assessment of the environment was conducted from September 16-19. The onsite assessment was conducted with full knowledge of the Federally Facilitated Marketplace and supporting infrastructure. This report contains the results of that effort.

The Federally Facilitated Marketplace staff provided Blue Canopy with excellent support during the engagement. Before the Blue Canopy Assessment Team arrived at the site, CGI Federal personnel provided Blue Canopy with various FFM system-related documents, including the SSP, ISRA, and CP documents. Developers, architects, and information security (IS) support personnel were interviewed and questions were answered promptly.

## 2.1 Assessment Methodology

Blue Canopy conducted its SCA of the Federally Facilitated Marketplace major application (MA) located at the NotResp

The purpose of this assessment was to do the following:

Ensure that the system was in compliance with the *CMS Information Security (IS) Acceptable Risk Safeguards (ARS),including CMS Minimum Security Requirements (CMSR), Version 1.5,* [2] *HHS Minimum Security Configuration Standards for Departmental Operating Systems*

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

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

*and Applications,*[3] *CMS Policy for the Information Security Program,*[4] and CMS *Business Partner Systems Security Manual, Version 10.6*[5].

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

[3] http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/is_baseline_configs.pdf (May 3, 2012).
[4] https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/PISP.pdf (August 31, 2010).
[5] http://www.cms.gov/manuals/downloads/117_systems_security.pdf (July 17, 2009).

# 3. DETAILED FINDINGS

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

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

## 3.1 Methodology for the Comprehensive Scope Application Security Control Assessment

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

- Vulnerabilities and their potential impact
- Weak system configuration settings that if not changed could compromise the CIA of system data
- Where established CMS security policies have not been followed

### 3.1.1 COMPREHENSIVE SCOPE APPLICATION VULNERABILITY ASSESSMENT

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

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

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

- Failure to comply with CMS security policies and procedures

### 3.1.2 TESTS AND ANALYSES

The comprehensive scope application SCA included a number of tests that methodically analyzed the FFM application. The types of tests and analyses Blue Canopy performed during this assessment included the following:

**Application Assessment**—subjected the thick-client applications to manual and automated testing to ensure the CIA of data processed by the application

**Best Engineering Judgment and Various Ad Hoc Tests**—verified that specific requirements, previous recommendations, and conditions had been satisfied

### 3.1.3 TOOLS

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

**Achilles** (http://www.mavensecurity.com/achilles)—tool designed for testing the security of Web applications

**Burp Suite** (http://portswigger.net/burp/)—integrated platform for performing security testing of web applications.

**Cookie Digger** (http://www.foundstone.com)—tool used to collect and analyze cookie values used to maintain session state and isolation by identifying the use of easily guessed or predictable cookie values

**Curl** (http://curl.haxx.se/)—open-source command line tool for transferring files with Uniformed Resource Locator (URL) syntax

**Httprint** (http://net-square.com/httprint/)—Web server fingerprinting tool

**Httrack** (http://www.httrack.com/)—open-source offline browser utility

**MetaCoretex** (http://sourceforge.net/projects/metacoretex/)—Java-based tool that provides a graphical user interface (GUI) and tests a number of different database systems

**Mozilla and Firefox Web Browsers** (http://www.mozilla.org)—open-source Web-based browsers used to manually browse and inspect the Web application and associated forms

**Netcat** (http://packetstormsecurity.nl/UNIX/netcat/)—open-source utility that reads and writes data across network connections using Transmission Control Protocol (TCP) or User Datagram Protocol (UDP)

**Nikto** (http://www.cirt.net/code/nikto.shtml)—open-source, command-line, Web server scanner

**Nmap** (http://www.insecure.org/nmap/)—open-source utility for network exploration or security auditing through UDP and TCP port scanning

**Paros** (http://www.parosproxy.org)—Java-based Web proxy tool used to evaluate Web application security (similar to Achilles)

**Openssl** (http://www.openssl.org/)—open-source library that provides cryptographic functionality to applications such as secure Web servers.

**Oracle Auditing Tools (OAT)** (http://www.cqure.net/wp/test/)—open-source command-line toolkit designed to enumerate an Oracle server and potentially execute commands on the server

**Oracrack** (http://www.0xdeadbeef.info/code/oracrack)—Oracle password hash cracking utility (dictionary + brute force)

**RAT** (http://www.cisecurity.org/)—open-source tool used to assess Cisco router Internetwork Operating System (IOS) and Cisco Private Internet EXchange (PIX) firewalls

**SiteDigger** (http://www.foundstone.com/)—tool that searches Google's cache to look for vulnerabilities, errors, configuration issues, proprietary information, and interesting security nuggets on Web sites

**SpikeProxy** (http://www.immunitysec.com/resources-freesoftware.shtml)—Web proxy that captures and replays Hyper Text Transfer Protocol (HTTP) packets with permuted input

**SQLplus**—used to access databases over a network connection in order to discover potential configuration errors

**SSLDigger** (http://www.foundstone.com/)—provides a GUI to a tool used to assess the strength of Secure Sockets Layer (SSL) servers by testing the supported cipher

**Stompy** (http://lcamtuf.coredump.cx)—open-source command line tool for Linux, which is used to collect and analyze cookie and URL parameter values used as session identifiers

**Stunnel** (http://www.stunnel.org)—universal SSL wrapper that allows the encryption of arbitrary TCP connections inside SSL

**WebScarab** (http://www.owasp.org/index.php/Category:OWASP_WebScarab_Project) —Java-based Web proxy tool used to evaluate Web application security

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

**Wireshark** (http://www.wireshark.org)—open-source, GUI network protocol analyzer

## 3.2 Methodology for Security Test Reporting

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

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

*Procedure for Information Security (IS) Assessments* document, Blue Canopy has assigned these values to each Business Risk.

### 3.2.1 RISK LEVEL ASSESSMENT

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

**Table 1. Risk Level Definitions**

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

### 3.2.2 EASE-OF-FIX ASSESSMENT

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

**Table 2. Ease-of-Fix Definitions**

| Rating | Definition of Risk Rating |
|---|---|
| Easy | The corrective action(s) can be completed quickly with minimal resources and without causing disruption to the system, or data |
| Moderately Difficult | Remediation efforts will likely cause a noticeable service disruption<br>• A vendor patch or major configuration change may be required to close the vulnerability.<br>• An upgrade to a different version of the software may be required to address the impact severity<br>• The system may require a reconfiguration to mitigate the threat exposure<br>• Corrective action may require construction or significant alterations to the manner in which business is undertaken |
| Very Difficult | The high risk of substantial service disruption makes it impractical to complete the corrective action for mission critical systems without careful scheduling<br>• An obscure, hard-to-find vendor patch may be required to close the vulnerability<br>• Significant, time-consuming configuration changes may be required to address the threat exposure or impact severity<br>• Corrective action requires major construction or redesign of an entire business process |
| No Known Fix | No known solution to the problem currently exists. The Risk may require the Business Owner to: |

| Rating | Definition of Risk Rating |
|---|---|
| | • Discontinue use of the software or protocol<br>• Isolate the information system within the enterprise, thereby eliminating reliance on the system<br>In some cases, the vulnerability is due to a design-level flaw that cannot be resolved through the application of vendor patches or the reconfiguration of the system. If the system is critical and must be used to support on-going business functions, no less than quarterly monitoring shall be conducted by the Business Owner, and reviewed by CMS IS Management, to validate that security incidents have not occurred |

### 3.2.3 ESTIMATED WORK EFFORT ASSESSMENT

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

**Table 3. Estimated Work Effort Definitions**

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

## 3.3 Business Risks

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

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

| 3.3.1. Business Risk | (b)(5) |
|---|---|

**Applicable Standards:**

**NIST Security Control Families:** Access Control

**Reference:** AC-6

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

Moderate

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

Easy

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

Minimal

**Description:**

3.3.1 HIX-A 09232013

***Finding***

(b)(5)

**Suggested Corrective Action(s):**

(b)(5)

**Status:**

Identified on 9/19/2013

| 3.3.2. Business Risk | NotResp |
|---|---|

**Applicable Standards:**

**NIST Security Control Families:** Access Control (AC)

**Reference:** AC-6

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

Moderate

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

Easy

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

Minimal

**Description:**

3.3.2 HIX-A 09232013

***Finding***

NotResp

## Suggested Corrective Action(s):

NotResp

## Status:

Identified on 9/18/2013

| 3.3.3. Business Risk | NotResp |
|---|---|

**Applicable Standards:**

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

**Reference:** SC-13

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

Moderate

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

Easy

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

Minimal

**Description:**

3.3.3 HIX-A 09232013

***Finding***

NotResp

**Suggested Corrective Action(s):**

NotResp

**Status:**

Identified on 9/18/2013

| 3.3.4. Business Risk | NotResp |
|---|---|

**Applicable Standards:**

**NIST Security Control Families:** Access Control

**Reference:** AC-3

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

Moderate

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

Moderate

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

Moderate

**Description:**

3.3.4 HIX-A 09272013

NotResp

NotResp

**Suggested Corrective Action(s):**

NotResp

**Status:**

Identified on 9/27/2013

| 3.3.5. Business Risk | NotResp |
|---|---|

**Applicable Standards:**

**NIST Security Control Families:** Access Control (AC)

**Reference:** AC-6

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

Low

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

Easy

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

Minimal

**Description:**

3.3.5 HIX-A 09232013

NotResp

## Suggested Corrective Action(s):

NotResp

## Status:

Identified on 9/18/2013

| 3.3.6. Business Risk | NotResp |
|---|---|

**Applicable Standards:**

**NIST Security Control Families:** Access Control (AC)

**Reference:** AC-6

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

Low

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

Easy

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

Minimal

**Description:**

3.3.6 HIX-A 09232013

NotResp

## Suggested Corrective Action(s):

NotResp

## Status:

NotResp

| 3.3.7. Business Risk | NotResp |
|---|---|

**Applicable Standards:**

**NIST Security Control Families:** Access Control (AC)

**Reference:** AC-6

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

Low

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

Moderate

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

Moderate

**Description:**

3.3.7 HIX-A 09232013

NotResp

## Suggested Corrective Action(s):

NotResp

## Status:

Identified on 9/18/2013

NotResp

| 3.3.8. Business Risk | NotResp |
|---|---|

**Applicable Standards:**

**NIST Security Control Families:** System and Communications Protection

**Reference:** SC-5

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

Low

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

Moderate

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

Moderate

**Description:**

3.3.8 HIX-A 09232013

NotResp

NotResp

## Suggested Corrective Action(s):

NotResp

## Status:

Identified on 9/18/2013

| 3.3.9. Business Risk | NotResp |
|---|---|

**Applicable Standards:**

**NIST Security Control Families:** System Integrity

**Reference:** SI-10

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

Low

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

Moderate

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

Moderate

**Description:**

3.3.9 HIX-A 09232013

NotResp

NotResp

**Suggested Corrective Action(s):**

NotResp

**Status:**

Identified on 9/18/2013

# 4. DOCUMENTATION LISTS

MITRE was the prime contractor on the HIX-A/FFM assessment and they managed all of the document requests and reviews for the FFM assessment. As such, Blue Canopy defers all document requests and tracking to MTIRE for this particular assessment.