
From: Park, Todd
Sent: Thursday, April 11, 2013 4:58 PM
To: VanRoekel, Steven
Subject: RE: Coordination on ACA

Hey brother, thanks so much for the note and the chat! Many apologies for not staying in tighter sync with you on this will make sure we stay in close sync going forward.

Laura is rescheduling the site visit to happen in the next week or two, and we're going to have our ACA Next Steps meeting tomorrow with our smaller circle of WH folks to discuss the red team results and recommendations further (you'll see how unflinchingly clear-eyed and paranoid the red team was, as red teams need to be!) and also to discuss the path forward on the interagency steering committee (which sounds like it has already evolved into its ideal form going forward).

And then separately, Laura is also setting up more 1 to 1 time for you and me to talk about how we optimally coordinate across our joint portfolio. As a hint of coming attractions, you're going to need to stay involved in ACA ☺

It is absolutely awesome to be your teammate, and I truly treasure the incredible collaboration -for-the-public-good we've forged across our offices, which I really do think of as a single team. May the double helix of awesomeness continue, and may the Force continue to be with us ☺

Todd

From: VanRoekel, Steven
Sent: Thursday, April 11, 2013 2:31 PM
To: Park, Todd
Subject: Coordination on ACA

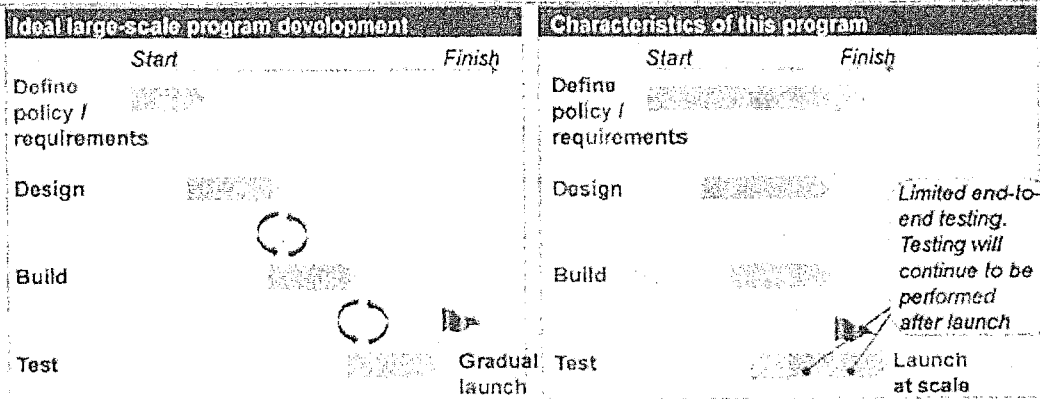
Todd, On ACA - I am hearing some feedback from both inside and outside the building about briefings to the President next week, coordination on a "Red Team" with CMS, suggestions that we cancel the steering committee meeting, suggestion that I not do a CMS visit tomorrow, and more. These raise concerns for me because when it's time to publicly deliver on ACA, I will be the one called to the Hill to testify and, per my statutory authority, will be held accountable for the successful delivery of this project. I anticipate there being increased Congressional scrutiny on the FFE as we move forward. This is just as critical to the legacy of many Congresspeople as it is to the President, and that will raise the likelihood of oversight hearings.

I am not trying to land grab in any way, I just worry that we are uncoordinated here, and that given your history and closeness with HHS, you are not hearing what I am hearing from the budget people in OMB, other agencies (other than CMS) and the private sector that CMS is not being inclusive and is not leading a coordinated effort that will lead to success. I am also worried that you getting a too-CMS-centric picture.

I would love nothing more than this not to be the case, to be assured ACA implementation is on a path we want it to be on, and that existing efforts will deliver what we want.

I think we should, as our next meeting on ACA, sit down, without staff, and have a 1:1 to talk about how we coordinate going forward.

Programs of this type ideally have a sequential planning, design, and implementation process with significant testing and revision



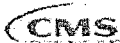
Description of ideal situation:

- Clear articulation of requirements & success metrics
- Minimized dependency on third parties
- Sequential requirements, design, build, and testing
- Iteration and revision between phases
- End-to-end integrated operations and IT testing
- Limited initial launch

Current situation:

- Evolving requirements
- Multiple definitions of success
- Significant dependency on external parties/contractors
- Parallel "stacking" of all phases
- Insufficient time and scope of end-to-end testing
- Launch at full volume

CMS has been working to mitigate challenges resulting from program characteristics



Centers for Medicare & Medicaid Services

[REDACTED]

From: Park, Todd [mailto:[REDACTED]]
Sent: Friday, August 23, 2013 11:18 AM
To: Chao, Henry (CMS/OIS)
Cc: Mielke, Dawn M.; Graubard, Vivian
Subject: Calling Red Hat

Hey brother, great to speak with you this morning – just wanted to let you know that I could be available to call Red Hat at 1 pm or between 3 to 4 pm.... Might that work for you? I get on a flight at 5 pm – but can totally delay that if needed.... Just let me know, thanks!

Todd

To: Coutts, Todd (CMS/OIS) ([REDACTED])
Cc: Calem, Mark (CGI Federal) ([REDACTED]); Weiss, Paul (CGI Federal) ([REDACTED])
From: Manambedu, Lakshmi (CGI Federal)
Sent: Fri 7/12/2013 6:11:47 PM
Subject: RE: Need a write up for Todd
Day One Capabilities - Priority and Risk - 20130712.docx

Hi Todd,

Attached is what I have for E&E. You may be able to extract the major ones from this.

In terms of other major milestones between Oct 1 and Jan 2014 are:

- Enrollment Reconciliation – December 2013
- Exemptions Applications – December 2013
- Payment to Issuers – 3rd week of January 2014

Thank you

Lakshmi Manambedu | Vice President, CGI Federal | Mobile: [REDACTED] www.cgi.com

From: Chao, Henry (CMS/OIS) [mailto:henry.chao@[REDACTED]]
Sent: Friday, July 12, 2013 12:58 PM
To: Manambedu, Lakshmi (CGI Federal); Kariton Kim (kkim@[REDACTED]); Donohoe, Paul X. (CMS/OIS); Coutts, Todd (CMS/OIS); Rhones, Rhonda D. (CMS/OIS)
Cc: Oh, Mark U. (CMS/OIS); Berkley, Katrina (CMS/OIS); Coutts, Todd (CMS/OIS); Rhones, Rhonda D. (CMS/OIS); Grothe, Kirk A. (CMS/OIS)
Subject: Need a write up for Todd
Importance: High

This is for sources material for Todd Park to pick nuggets from in his prep for briefing POTUS next week.

So the write-up which are sentence(s) in bullet format needs to cover:

- The A-Z of testing by partner (Issuer, # of Issuers, State programs, types of Marketplace, approach (waves, harness, DE, 834/enrollment, etc.), and high level schedule.

- Overall list of key activities to be accomplished and risks for Day one (remaining 80 days) and Day ones for other major lifts prior to Day one of the benefit and the start of the benefit.

Please use material we have already like the deck that we used for SVR and updated another version for Marilyn/OL a few days ago.

Remember that bullets should not be written to be used to create more questions.

Rhonda and Todd—please collect, format, and send to me by COB today.

Henry Chao

Deputy CIO & Deputy Director,

Office of Information Services

Centers for Medicare & Medicaid Services

██████████

██████████

From: Snyder, Michelle (CMS/OA) <[REDACTED]>
Sent: Sunday, September 29, 2013 6:22 PM
To: Park, Todd
Subject: Re: Discussion points

Just so you know she decided in January we were going no matter what - hence the really cruel and uncaring march that has occurred since January when she threatened me with a demotion or forced retirement if I didn't take this on - do you really think she has enough understanding of the risks to fight for a delay - no and hell no - for just one moment let's be honest with each other. I appreciate your belief in the goodness of others but at this point I am too tired to pretend there is a decision to be made - it is just how much crap my team will have to take if it isn't sufficiently successful - you haven't lived through the temper tantrums and threats for the last 9 months.

OK - that felt good - - am now back to my role as no comment civil servant

Delete this after reading - promise

M

Sent from my BlackBerry Wireless Device

----- Original Message -----

From: Park, Todd [mailto:[REDACTED]]
Sent: Sunday, September 29, 2013 05:54 PM
To: Snyder, Michelle (CMS/OA)
Subject: RE: Discussion points

Yes, got it. On the call with MT, Chris, and Jeanne, MT said that she appreciates the additional info we will generate tonight, but that she and she alone will make the decision to go or not - which of course is right. And the way she is thinking about it from a performance standpoint is that if enough of the additional hardware gets online to give us an insurance policy, she is comfortable proceeding, with 90,000 concurrent users being far beyond the 50,000 that was the CMS target.

Because new hardware is going live on a rolling basis today and tomorrow, I think we are in very good shape on the hardware front - and because the Miami equipment got here so early today, we've got a good shot at that being live and helping us get to 90,000.

Will be good tonight as per one of the questions for the 9 pm to get people's guesstimate of what kind of traffic in general (order of magnitude) would be associated with a 90,000 concurrent user scenario, just so MT has that.

And will also be good to understand the EIDM situation a bit better to see if that is a separate bottleneck with a lower concurrent user threshold? And if that's a possible threat to monitor. Again, just to inform MT.

Going to deliver cupcakes now :)

-----Original Message-----

From: Snyder, Michelle (CMS/OA) [mailto:[REDACTED]]

Because new hardware is going live on a rolling basis today and tomorrow, I think we are in very good shape on the hardware front – and because the Miami equipment got here so early today, we've got a good shot at that being live and helping us get to 90,000.

Will be good tonight as per one of the questions for the 9 pm to get people's guesstimate of what kind of traffic in general (order of magnitude) would be associated with a 90,000 concurrent user scenario, just so MT has that.

And will also be good to understand the EIDM situation a bit better to see if that is a separate bottleneck with a lower concurrent user threshold? And if that's a possible threat to monitor. Again, just to inform MT.

Going to deliver cupcakes now :)

-----Original Message-----

From: Snyder, Michelle (CMS/OA) [mailto: [REDACTED]]
Sent: Sunday, September 29, 2013 4:02 PM
To: Park, Todd
Subject: Re: Discussion points

These are helpful but we are going live one way or another. MT has made it clear to me that that question isn't on the table. It is more knowing how to message what won't work

M

Sent from my BlackBerry Wireless Device

----- Original Message -----

From: Park, Todd [mailto: [REDACTED]]
Sent: Sunday, September 29, 2013 02:42 PM
To: Snyder, Michelle (CMS/OA)
Subject: Fw: Discussion points

Hi M, just sending this to you so I don't distract folks in mid-flight this afternoon. On load/performance, it will be very helpful at the end of the day for you to do a gutcheck -- with Henry and Dave and whomever else they'd like to include (I'm happy to join as well) -- to net out where we are, make an educated guess about what is likely to happen on Oct 1, and recommend to Marilyn that we go/no go. I'm sure you have already thought this through, but here's a sample "logic path" to talk through with Henry/Dave and team, building on the questions from the earlier email (I know you're hyperfocused on other items like call center right now, so I thought I might prep this for you at least as a draft):

-- Does the performance testing that the team has done give you confidence that the FFM can handle 21,000 concurrent users with existing hardware and about 90,000 concurrent users with the new hardware added -- with great user response times? What might the holes be in terms of our knowledge of system performance?

-- Where are we in the installation and activation of the new hardware? How confident are we that all of it will be online and ready by Monday COB?

-- Confirm that the 90,000 concurrent user figure means that literally 90,000 people can be hitting the exact same keystrokes, doing the exact same thing, stressing out the exact same precise part of the FFM, at the exact same time

-- Confirm that what for sure doesn't impact the FFM's functionality or access is if there happens to be a zillion of her people hitting the homepage/"Learn about the Marketplace" pages on HealthCare.gov at that same moment, because it's technically separate from the Get Insured workflow. (And you should confirm that the homepage/"Learn" pages on HC.gov are ready for an onslaught (including Akamai caching))

-- Question: while 90,000 users in the FFM functionality itself are all doing the exact same thing to the FFM in a single unified punch at the same millisecond, what can other users in the FFM workflow be doing? Can many others be "in between" clicks i.e., reading a page, filling out fields on a webpage before hitting submit, surveying their plan options? What is our even rough intuitive sense about if others can also be actively exercising different parts of the FFM different clicks on different functionality?

-- Based on the above and what we might guesstimate about Day 1 use patterns, what kind of overall total FFM user volume for Day 1 do we think is supportable if we can support 90,000 concurrent FFM workflow users? (This is obviously going to be a swag, because it's hard to predict distribution of visits over the course of the day, but Dave/Henry may have some instincts about this based on past experience)

-- What happens after the 90,000 concurrent user threshold is reached? Is there gradual degradation of response time for users? Rapid degradation? Immediate crashing?

-- What is your best professional gut guess (based both on what you know and don't know) as to the percentage probability that the system will slow to unacceptable levels of performance, or crash entirely? (They may only really be able to give you a qualitative sense of this)

-- Should we go live on Oct 1?

Again, just a suggestion/draft as to the logic path -- feel free to shred/add items/delete items/change entirely :)

----- Original Message -----

From: Park, Todd

Sent: Sunday, September 29, 2013 10:27 AM

To: Snyder, Michelle (CMS/OA) <[REDACTED]>; Chao, Henry (CMS/OIS) <[REDACTED]>;

Bowen, Marianne (CMS/OA) <[REDACTED]>

Subject: RE: Discussion points

Hi Michelle, as your consigliere, I do recommend that you ask the questions below -- which are of course questions that Henry is already asking himself, but it would be good for you to know the answers as well :)

And Henry, needless to say: work to actually continually make key things better takes absolute precedence over question answering :)

And again, the only questions you should answer are from Michelle :) I've added her additional question and put it at the top of the recapped list below (and have also adjusted the numbers based on the update). She can pick from #2 through #6 below and designate which ones she really cares about :)

And I've taken a shot at answering some of them (#2, #4, #5) based on my understanding from the brief discussion this morning -- which Henry can correct as necessary:

(1) Would it help to have someone like NGS help with the testing on an ongoing basis?

A:

From: Park, Todd
Sent: Sunday, September 29, 2013 7:13 PM
To: 'Michelle.Snyder [REDACTED]
Subject: Re: Discussion points

M, I think (knock on wood!!!!!!) that you and team are actually going to pull off the feat of the century -- a feat that will go down in history, and literally change the course of history for the better. No other team could have possibly come close to what you've done and are doing. No one.

We all as Americans owe you and team an extraordinary debt of gratitude -- for your incredible ingenuity, your deep sacrifice, your superhuman level of effort and focus, your extraordinary tenacity. You have my word that I will continue to do everything in my power to make sure everyone understands this in the months and years ahead. I know y'all are not chest-thumpers -- that's part of what I love about all of you -- but I really do think that it's important for folks to understand how absolutely incredible you and team are, and I will continue to spread that understanding.

Please don't ever hesitate to ask me for anything I can do to be helpful on this or any other front -- and if there is any way for me to help celebrate the team -- whether it be cupcakes :) or a meeting with POTUS (which I will start working on)

Semper fi, and much love,
Todd

----- Original Message -----

From: Snyder, Michelle (CMS/OA) [mailto:[REDACTED]]
Sent: Sunday, September 29, 2013 07:03 PM
To: Park, Todd
Subject: Re: Discussion points

And I have kept this all from my team. Marianne and Jim and Andi know about how bad it has been. The rest need the illusion - the four of us have none left

M

Sent from my BlackBerry Wireless Device

----- Original Message -----

From: Park, Todd [mailto:[REDACTED]]
Sent: Sunday, September 29, 2013 05:54 PM
To: Snyder, Michelle (CMS/OA)
Subject: RE: Discussion points

Yes, got it. On the call with MT, Chris, and Jeanne, MT said that she appreciates the additional info we will generate tonight, but that she and she alone will make the decision to go or not -- which of course is right. And the way she is thinking about it from a performance standpoint is that if enough of the additional hardware gets online to give us an insurance policy, she is comfortable proceeding, with 90,000 concurrent users being far beyond the 50,000 that was the CMS target.

Message

From: Tavenner, Marilyn (CMS/OA) [/O=HHS EES/OU=FIRST ADMINISTRATIVE GROUP/CN=RECIPIENTS/CN=MARILYN.TAVENNER.CMS]
Sent: 6/26/2013 9:55:47 PM
To: 'Todd_Y_Park [REDACTED]'; Snyder, Michelle (CMS/OA) [/O=HHS EES/OU=First Administrative Group/cn=Recipients/cn=Michelle.Snyder.CMS]; Chao, Henry (CMS/OIS) [/O=HHS EES/OU=First Administrative Group/cn=Recipients/cn=Henry.Chao.OS]
CC: Khalid, Aryana C. (CMS/OA) [/O=HHS EES/OU=First Administrative Group/cn=Recipients/cn=Aryana .Khalid .CMS]
Subject: Re: Follow-up

Thanks Todd. Appreciate the help as always!!!!

From: Park, Todd [mailto:[REDACTED]]
Sent: Wednesday, June 26, 2013 05:34 PM
To: Tavenner, Marilyn (CMS/OA); Snyder, Michelle (CMS/OA); Chao, Henry (CMS/OIS)
Subject: Follow-up

Hi Marilyn, Michelle, and Henry,

After talking with Henry and team, I spoke with Mark about the logo issue, and explained why attempting to add logos for October 1 is extremely unwise. He understands. He may want me to get on the phone with someone from the Blues so they fully understand it. I'm more than happy to do so on your behalf – this issue should not consume any more of your time.

Marilyn, I'm also going to visit with Henry and team for one of our evening deep-dive sessions to get up to speed on the latest status of IT and testing – during the week of July 8. Michelle, Henry, and I had a check-in call today, but I think that Henry is right that to really understand current status and next steps, there is no substitute for an evening deep-dive. So I'll bring healthy food and snacks to Baltimore and camp out with Henry and team for a few hours ☺

All the best,
Todd

Both Julian and David took great pains to ask that the visit not be disruptive to your work -- I think that the message to give y'all the space to rock and roll is spreading :)

So I'm thinking a focused two-hour visit, in Baltimore, going thru the live workflow, and using high-level materials you already have.

Would next week be best, or would the week after be better, or would either week be fine? I haven't yet pinged David and Julian for their availability, but wanted to see what was optimal for you first. It would be good to combine both of their visits, to save you time. Thoughts on timing?

Michelle, it would be terrific for you to join -- would be great for you to meet Julian and David, both of whom are terrific; and I've told both of them that you and Henry are pure awesomeness :)

Thanks!
Todd

----- Original Message -----

From: Chao, Henry (CMS/OIS) [REDACTED]
Sent: Thursday, July 25, 2013 09:53 AM
To: Park, Todd
Cc: Oh, Mark U. (CMS/OIS) [REDACTED] Coutts, Todd (CMS/OIS)
[REDACTED] Outerbridge, Monique (CMS/OIS)
[REDACTED]; Grothe, Kirk A. (CMS/OIS)
[REDACTED] Berkley, Katrina (CMS/OIS)
[REDACTED]; Rhones, Rhonda D. (CMS/OIS)
[REDACTED]; Graubard, Vivian;
[REDACTED] <rich.martin@[REDACTED]>;
'cheryl.campbell@[REDACTED]>;
'Lakshmi.Manambedu@[REDACTED]>;
'Mark.Calem@[REDACTED]>;
'Paul.Weiss@[REDACTED] Wallace, Mary H.
(CMS/OC) [REDACTED]; Booth, Jon G. (CMS/OC)
[REDACTED]

Todd,

If you recall we had agreed to provide you a walk through and demo of the online application in its current form so you can get a chance to peek under the covers of hc.gov.

Key Points Discussed		
No.	Topic	Highlights
2	Workgroup Updates	<p>dependencies from consent.</p> <p>Marilyn Tavenner has been engaged in the consent resolution conversations.</p> <ul style="list-style-type: none"> • Details cannot be flushed out until these conversations are complete. • CMS has been ordered to await the completion of these discussions before determining the necessary changes to the baseline schedule. <p>Todd Park has been engaged in discussion on NIST Level 2 inter-mechanics.</p> <ul style="list-style-type: none"> • CMS is moving forward with following this process, which represents SSA's understanding, as well. • SSA is interested in understanding the downstream impact on the overall integrated testing, as well as the timeline. <p>Scheduling</p> <ul style="list-style-type: none"> • Highest risk to implementation associated with awaiting the high-level decision, as opposed to building for the worst case scenario: <ul style="list-style-type: none"> ○ Broad risk: Schedule and implementation risks would be the largest concerns. The schedule presents a risk of a 2-4 week delay. ○ The team must agree that the schedule risk is a priority and must find ways to retrieve the lost time from other areas. ○ It is unclear as to whom the Secretary is in discussion with or what the status of the discussion is. ○ Teams thought there would be simultaneous development between the legal issue and the IT build as the higher level issues were being addressed. The interagency team is not in full agreement on this issue. ○ David Black would like the teams to continue making technology progress. <p>Clarification: Identification Proofing vs. Consent</p> <ul style="list-style-type: none"> • Consent is a legal issue, whereas, identity proofing is a solution and process that needs to be established. • SSA is relying on the Privacy Act for legal authority on ID proofing as there is none provided in the Act. <ul style="list-style-type: none"> ○ Legal team is currently working this issue. ○ Identity proofing would be built in as a process for verifying an individual's identity. • Previous decision to use two IRS challenge questions at the threshold has been reconsidered and is currently being discussed. • Suggestion: A smaller group of key individuals may need to reconvene on this topic in 3-4 weeks including Marilyn because of her involvement with the scheduling. <p>Integrated Project Plan</p> <ul style="list-style-type: none"> • The IPP needs to be addressed before focusing on the schedule

<Brian.Cook@ [REDACTED] 'Michelle.Snyder@ [REDACTED]>
Subject: RE: Preventing Fraud in Marketplaces - WH background call with media tomorrow?

Thanks Todd – if your team could draft the cyber talking points, that would be very helpful. Thanks so much.

We are still working on finalizing the paper but will share those with everyone as soon as they are ready.

From: Park, Todd
Sent: Tuesday, September 17, 2013 7:22 PM
To: Santillo, Jessica; 'tony.trenkle@ [REDACTED]
Cc: Jones, Isabel; Mielke, Dawn M.; 'frank.baitman@ [REDACTED] 'Brian.Cook@ [REDACTED] 'Michelle.Snyder@ [REDACTED]
Subject: Re: Preventing Fraud in Marketplaces - WH background call with media tomorrow?

Thanks, Jessica. Tony and Frank, can you join via phone? You'll only be asked to help with the cybersecurity part of the call :) I am more than happy to deliver the primary talking points, which will focus principally on Marilyn's letter regarding Hub cybersecurity + the general points the three of us hammered out a while back.

Jessica, are you putting together talking points for us, or would you like me to take a crack at them?

Thanks,
Todd

From: Santillo, Jessica
Sent: Tuesday, September 17, 2013 07:13 PM
To: Park, Todd; Trenkle, Tony (CMS/OIS) < [REDACTED] >
Cc: Jones, Isabel; Mielke, Dawn M.; Baitman, Frank (OS/ASA/OCIO) < [REDACTED] > Cook, Brian T. (CMS/OC) < [REDACTED] >; Snyder, Michelle (CMS/OA) < [REDACTED] >
Subject: RE: Preventing Fraud in Marketplaces - WH background call with media tomorrow?

Hi Todd – happy to have Tony and Frank join us for the cyber security portion.

On your first question – the call is on background according to “White House officials.”

Thanks very much for making this work on such short notice. We will hold the call in EEOB 207. I will send around a calendar invite.

Thank you again,
Jessica

From: Park, Todd
Sent: Tuesday, September 17, 2013 6:14 PM
To: Trenkle, Tony (CMS/OIS); Santillo, Jessica
Cc: Jones, Isabel; Mielke, Dawn M.; Baitman, Frank (OS/ASA/OCIO); Cook, Brian T. (CMS/OC); Snyder, Michelle (CMS/OA)
Subject: RE: Preventing Fraud in Marketplaces - WH background call with media tomorrow?

From: Fasching, Laura <[REDACTED]>
Sent: Saturday, September 28, 2013 10:47 PM
To: Park, Todd; Chao, Henry (CMS/OIS)
Cc: Fasching, Laura
Subject: RE: How serious are you about using Homestead AFB to get the equipment to Culpeper?

Glad to help, let me know if you need anything else gentlemen ☺
Laura

Laura Fasching
Director of Public Sector Strategic Accounts | Verizon Terremark
Tel: [REDACTED]
222 W Las Colinas Blvd, Irving, Texas, 75039

From: Park, Todd [mailto:[REDACTED]]
Sent: Saturday, September 28, 2013 10:38 PM
To: Fasching, Laura; Chao, Henry (CMS/OIS)
Subject: RE: How serious are you about using Homestead AFB to get the equipment to Culpeper?

That is super-awesome Laura, thanks so very, very, very much!!!!

From: Fasching, Laura [mailto:[REDACTED]]
Sent: Saturday, September 28, 2013 10:36 PM
To: Chao, Henry (CMS/OIS); Park, Todd
Cc: Fasching, Laura
Subject: RE: How serious are you about using Homestead AFB to get the equipment to Culpeper?

Todd & Henry,

The shipper is picking up the equipment in the next 90 minutes from the Miami data center and we expect the shipment to arrive between 9:30 AM to 10:00 AM. ☺

So Monday COB is looking good as long as we keep the shippers on schedule, as the build teams will be working at 6 am with the equipment that was brought in today.

Laura

Laura Fasching
Director of Public Sector Strategic Accounts | Verizon Terremark
Tel: [REDACTED]
222 W Las Colinas Blvd, Irving, Texas, 75039

From: Chao, Henry (CMS/OIS) [mailto:[REDACTED]]
Sent: Saturday, September 28, 2013 9:03 PM
To: Fasching, Laura; Todd Y Park [REDACTED]
Subject: Re: How serious are you about using Homestead AFB to get the equipment to Culpeper?

I got the approval from our COO and head of Contracts to go with the 40k option.

Contracts said we will have to work out how this can be a line you can bill in the contract but no problem figuring that out later.

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

[REDACTED] (Pri)
[REDACTED] (Alt)
[REDACTED] (BB)

From: Fasching, Laura [mailto:[REDACTED]]
Sent: Saturday, September 28, 2013 09:00 PM
To: Park, Todd <[REDACTED]>; Chao, Henry (CMS/OIS)
Cc: Fasching, Laura <[REDACTED]>
Subject: RE: How serious are you about using Homestead AFB to get the equipment to Culpeper?

Ok great Henry can I get confirmation that the Government will Pay for the plane? We have to get David Small's Approval so we will need to call him as soon as possible.

Thanks and sorry to rush you all.

Laura

Laura Fasching
Director of Public Sector Strategic Accounts | Verizon Terremark
Tel: [REDACTED]
222 W Las Colinas Blvd, Irving, Texas, 75039

From: Park, Todd [mailto:[REDACTED]]
Sent: Saturday, September 28, 2013 8:50 PM
To: Fasching, Laura; Chao, Henry (CMS/OIS)
Subject: RE: How serious are you about using Homestead AFB to get the equipment to Culpeper?

FYI, the private plane option I am pursuing would likely cost about the same as the Fedex expedite cargo plane option below.

Henry, I think that delivery to the data center mid -day Sunday sounds really, really, really good...

From: Fasching, Laura [mailto:[REDACTED]]
Sent: Saturday, September 28, 2013 8:46 PM
To: Park, Todd; Chao, Henry (CMS/OIS)
Cc: Fasching, Laura
Subject: RE: How serious are you about using Homestead AFB to get the equipment to Culpeper?
Importance: High

Ok here is what I was able to do
I was able to get to FedEx custom Critical they can drive it to us via a truck with pick up tonight @ 11:00 PM (ish) and delivery around 9 PM on Sunday night for \$3700.00
Or

To: Chao, Henry (CMS/OIS); Fasching, Laura
Subject: RE: How serious are you about using Homestead AFB to get the equipment to Culpeper?

Laura, by when do you need to make a decision about whether to send via private ground, private cargo plane, or Air Force (if Air Force is indeed an option?)

And to confirm private ground would deliver the hardware on Tuesday (to be installed Wednesday?), private cargo plane would deliver the hardware on Monday (to be installed Tuesday?). With no possibility of acceleration of those timetables?

From: Chao, Henry (CMS/OIS) [mailto: [REDACTED]]
Sent: Saturday, September 28, 2013 7:29 PM
To: 'laura.fasching [REDACTED]'; Park, Todd
Subject: Re: How serious are you about using Homestead AFB to get the equipment to Culpeper?

Todd--it's in your hands now to make a quick decision.

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

[REDACTED] (Pri)
[REDACTED] (Alt)
[REDACTED] (BB)

From: Fasching, Laura [mailto: [REDACTED]]
Sent: Saturday, September 28, 2013 07:27 PM
To: Park, Todd < [REDACTED] >; Chao, Henry (CMS/OIS)
Subject: RE: How serious are you about using Homestead AFB to get the equipment to Culpeper?

We have been exploring that option too but no luck so far

Laura Fasching
Director of Public Sector Strategic Accounts | Verizon Terremark
Tel: [REDACTED]
222 W Las Colinas Blvd, Irving, Texas, 75039

From: Park, Todd [mailto: [REDACTED]]
Sent: Saturday, September 28, 2013 7:26 PM
To: Chao, Henry (CMS/OIS); Fasching, Laura
Subject: RE: How serious are you about using Homestead AFB to get the equipment to Culpeper?

Also: as another option to explore, in the interest of exploring all options simultaneously, is it possible to arrange for heroic chartered private sector ground transportation that could get going super -early tomorrow morning and get to Culpeper by Sunday evening?

From: Park, Todd
Sent: Saturday, September 28, 2013 7:03 PM

To: 'Chao, Henry (CMS/OIS)'; 'laura.fasching [REDACTED]
Subject: RE: How serious are you about using Homestead AFB to get the equipment to Culpeper?

WH team responded instantly, is working on it as we speak and will get back to us ASAP. But they unfortunately are not optimistic, so we should explore other options in parallel.

Is there any possibility of arranging for private/commercial cargo plane transport? Chartered, even?

From: Chao, Henry (CMS/OIS) [mailto:[REDACTED]]
Sent: Saturday, September 28, 2013 6:36 PM
To: 'laura.fasching [REDACTED]
Cc: Park, Todd
Subject: Re: How serious are you about using Homestead AFB to get the equipment to Culp eper?

Just talked to Todd and he is going to talk to the rest of WH that can make this happen so just reply with the confirmed service to Homestead.

Todd--let us know ASAP so laura will send via ground if you can't arrange for transport to someplace the Air Force can land near Culpeper VA.

Henry Chao
Deputy Chief Information Officer and Deputy Director
Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Blvd
Baltimore, MD 21244
[REDACTED] (Pri)
[REDACTED] (Alt)
[REDACTED] (BB)

From: Fasching, Laura [mailto:[REDACTED]]
Sent: Saturday, September 28, 2013 06:09 PM
To: Chao, Henry (CMS/OIS)
Cc: Fasching, Laura <[REDACTED]>
Subject: RE: How serious are you about using Homestead AFB to get the equipment to Culpeper?

Henry,

We are working on firming up the white glove shippers but once that is done we would be good to go.

If we get the shippers scheduled and the equipment gets here tomorrow my engineers said they have the resources to build it out and just like we said before up by cob Monday.

I will let you know about the shippers within an hour.

Laura

Laura Fasching
Director of Public Sector Strategic Accounts | Verizon Terremark
Tel: [REDACTED]
222 W Las Colinas Blvd, Irving, Texas, 75039

From: Fasching, Laura <[REDACTED]>
Sent: Tuesday, October 01, 2013 2:08 AM
To: Park, Todd; Chao, Henry (CMS/OIS); Small, David (David); Drumgoole, Christopher R; michelle.snyder [REDACTED]
Cc: Um, Peter (CMS/CTR); Sharma, Hemant (CGI Federal) ([REDACTED]); Oh, Mark U. (CMS/OIS); Thurston, Robert (CMS/CTR); Fasching, Laura
Subject: RE: New expansion

Todd & Henry

As we have been working with your team to assist you in making the Marketplace launch successful, we continue to work to adapt to your needs.

Right now, I understand that while we add more compute, the team needs the VMs built faster.

In this tasking we are using the best practices that were agreed to as to not induce risk into your builds

- such as utilizing the kickstart process (custom templates of the hardened images) for RHEL 5 & 6; Windows VMs the SQL VMs utilizes a standard image which requires additional time to harden to NIST standards.

However we have found that due to the size of this environment 1500 + VMs, we are seeing an impact to running too many builds at once. As doing too builds at once slows down the process by overwhelming the Virtual Center server.

The options we have to increase the speed of the VM builds introduce a **SIGNIFICANT RISK** to the environment. We do not suggest either of these options, but I wanted to give you a full picture of the situation.

1. VC Client Basically cloning of existing VMs and while this may seem an easy option
 - a. Old network configs and FW rules have to be removed first. Then the new ones need to be done. very time consuming and manual
 - b. Finally, these VMs will not appear in iCenter. Without them being visible in iCenter, these VMs will be unmanageable in the future & you will not be able to manage the compute resources.
2. VM import may get the VM's in place but they have the exact same issues as noted above.

We have engaged our vendor URS to increase staffing during this time, and will follow up shortly on the results of that endeavor. If we can get a couple more people in now it will assist with allowing some team members to focus on the builds while other field calls and assist with troubleshooting.

Just as we did yesterday when we receive an request for more storage resources than were in either the reserve capacity or in the expansion order. We will work to adapt to your needs during as you bring the Affordable Care Act's Insurance Exchanges to the American public.

Thanks
Laura

Laura Fasching
Director of Public Sector Strategic Accounts | Verizon Terremark
Tel: [REDACTED]
222 W Las Colinas Blvd, Irving, Texas, 75039



Administrator
Washington, DC 20201

SEP 10 2013

The Honorable Bennie Thompson
Ranking Member
Committee on Homeland Security
U.S. House of Representatives
Washington, DC 20515

Dear Representative Thompson:

Thank you for your inquiry related to privacy and security protections associated with the Data Services Hub (Hub) and the status of our work to protect people and programs from cyber-attacks in this area. At the Department of Health and Human Services (HHS), we take very seriously our responsibility to safeguard personal information in all of our programs, including in the Affordable Care Act Marketplace. Collectively, the tools, methods, policies, and procedures we have developed provide a safe and sound security framework to safeguard consumer data, allowing eligible Americans to confidently and securely enroll in quality affordable health coverage starting on October 1, 2013. This framework is consistent with the framework that exists for all other HHS programs, such as Medicare, which Americans rely on every day.

HHS's Centers for Medicare & Medicaid Services (CMS) has a strong track record of preventing breaches involving the loss of personally identifiable information from cyber-attacks. This is due in large part to the establishment of an information security program with consistent risk management, security controls assessment, and security authorization processes for all enterprise systems. Our system and security protocols are grounded in statutes, guidelines and industry standards that ensure the security, privacy, and integrity of our systems and the data that flow through them. These protections include a series of statutes and amendments to these laws, such as the Privacy Act of 1974, the Computer Security Act of 1987 and the Federal Information Security Management Act (FISMA) of 2002, as well as various regulations and policies promulgated by HHS, the Office of Management and Budget, the Department of Homeland Security, and the National Institute of Standards and Technology (NIST).

In accordance with these provisions, CMS has developed the Hub, a routing tool that helps Marketplaces provide accurate and timely eligibility determinations. **It is important to point out that the Hub will not retain or store Personally Identifiable Information.** Rather, the Hub is a routing system that CMS is using to 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 with which we are validating data. These include the Social Security Administration, the Internal Revenue Service, the Department of Homeland Security, the Department of Veterans Affairs, Medicare, TRICARE, the Peace Corps and the Office of Personnel Management.

The Hub is designed to comply with the comprehensive information security standards developed by NIST in support of FISMA. NIST has emerged as the gold standard

for information security standards and guidelines that all federal agencies follow. Several layers of protection will be in place to help protect against potential damage from attackers and mitigate risks. For example, the Hub 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 potential attacks. Automated methods will ensure that system administrators have access to only the parts of the system that are necessary to perform their jobs. These protocols, combined with continuous monitoring, will alert system security personnel when any system administrator attempts to perform functions or access data for which they are not authorized or are inconsistent with their job functions.


Should security incidents occur, an Incident Response capability built on the model developed by NIST would be activated. The Incident Response function allows for the tracking, investigation, and reporting of incidents so that HHS may quickly identify security incidents and ensure that the relevant law enforcement authorities, such as the HHS Office of Inspector General Cyber Crimes Unit, are notified for purposes of possible criminal investigation.

Before Marketplace systems are allowed to operate and begin serving consumers across the country, they must comply with the rigorous standards that we apply to all federal operational systems and CMS's Chief Information Officer must authorize the systems to begin operation. I am pleased to report that the Hub completed its independent Security Controls Assessment on August 23, 2013 and was authorized to operate on September 6, 2013. The completion of this testing confirms that the Hub comports with the stringent standards discussed above and that HHS has implemented the appropriate procedures and safeguards necessary for the Hub to operate securely on October 1.

The privacy and security of consumer data are a top priority for HHS and our federal, state, and private partners. We understand that our responsibility to safeguard our systems is an ongoing process, and that we must remain vigilant throughout their operations to anticipate and protect against evolving data security threats. Accordingly, we have implemented privacy and security measures for the Marketplace systems that employ measures similar to those in the private sector and we will continually validate through a variety of methods.

In closing, we have produced an extremely strong enterprise information security program by implementing state-of-the-art controls and business processes based on statutory requirements, agency and organizational commitments, best practices, and the experience and knowledge of our subject matter team members. This has resulted in the development, testing and readiness of the Hub to operate on October 1 to serve consumers across the country in a secure and efficient manner. We hope this information is responsive to your inquiry. Thank you for your interest in and leadership on this important issue.

Sincerely,



Marilyn Tavenner

From: Russell,DeLaine <[REDACTED]>
Sent: Wednesday, September 11, 2013 11:10 AM
To: Trenkle, Tony (CMS/OIS)
Cc: Park, Todd; Cook, Brian T. (CMS/OC); Aronson, Lauren (CMS/OL); Snyder, Michelle (CMS/OA); Baitman, Frank (OS/ASA/OCIO); Fryer, Teresa M. (CMS/OIS); Mellor, Michael (CMS/OIS)
Subject: RE: Gartner

Tony,
Thank you for sending the letter. I have identified Gartner analyst Christian Byrnes, who will review and provide comment. Christian is a managing vice president at Gartner. His team is distributed across the globe and covers the management of risk-related programs such as Information Security, Business Continuity, Privacy and Compliance. In addition, he confers with leading organizations worldwide on technology direction, security trends and best practices. I will provide his response as soon as possible.

DeLaine

DeLaine Russell | Vice President - Public Sector | Gartner, Inc. | 4501 N. Fairfax Dr. | Arlington, VA 22203 | U.S.A. |
Office: +[REDACTED] | Fax: +[REDACTED] | Mobile: +1 [REDACTED] | Email: [REDACTED] |
www.gartner.com

P Please consider our environment before printing

-----Original Message-----

From: Trenkle, Tony (CMS/OIS) [mailto:[REDACTED]]
Sent: Wednesday, September 11, 2013 11:00 AM
To: Russell,DeLaine
Cc: Park, Todd; Cook, Brian T. (CMS/OC); Aronson, Lauren (CMS/OL); Snyder, Michelle (CMS/OA); Baitman, Frank (OS/ASA/OCIO); Trenkle, Tony (CMS/OIS); Fryer, Teresa M. (CMS/OIS); Mellor, Michael (CMS/OIS)
Subject: FW: Gartner

Hi DeLaine,

Per our conversation here is the letter that went to the Committee. Please let us know what your analysts' thoughts are.

Thanks.

Tony

>-----Original Message-----

>From: Aronson, Lauren (CMS/OL)
>Sent: Wednesday, September 11, 2013 9:12 AM
>To: Park, Todd; Trenkle, Tony (CMS/OIS)
>Cc: Cook, Brian T. (CMS/OC); Snyder, Michelle (CMS/OA)
>Subject: RE: Gartner
>
>Here's the final signed letter.

From: Trenkle, Tony (CMS/OIS) [mailto: [REDACTED]]
Sent: Thursday, September 12, 2013 08:49 AM
To: Park, Todd
Cc: Baitman, Frank (OS/ASA/OCIO) < [REDACTED] >; Fryer, Teresa M. (CMS/OIS) < [REDACTED] >; Mellor, Michael (CMS/OIS) < [REDACTED] >
Subject: FW: Comment from Gartner Analyst Christian Byrnes

Todd,

Does this help?

Tony

From: Russell, DeLaine [mailto: [REDACTED]]
Sent: Wednesday, September 11, 2013 12:04 PM
To: Trenkle, Tony (CMS/OIS)
Cc: Helliger, Christopher
Subject: Comment from Gartner Analyst Christian Byrnes

Tony,

Below is what I just received from the analyst. I hope this is what you are looking for. Chris is our most knowledgeable and experienced information security analyst.


Best,
DeLaine

Gartner Inc advises thousands of enterprise and government clients on best practices associated with the use of information technology. As a leader of the information security practice within Gartner Research I certify that the statements made in this letter represent current best practices for the protection of sensitive and regulated data and systems.

—
F. Christian Byrnes
Managing Vice President, Risk and Security Program Management
Gartner Inc.

[REDACTED]

DeLaine Russell | Vice President - Public Sector | Gartner, Inc. | 4501 N. Fairfax Dr. | Arlington, VA 22203 | U.S.A. | Office: + [REDACTED] | Fax: + [REDACTED] | Mobile: +1 [REDACTED] | Email: [REDACTED] | www.gartner.com

 Please consider our environment before printing

This e-mail message, including any attachments, is for the sole use of the person to whom it has been sent, and may contain information that is confidential or legally protected. If you are not the intended recipient or have received this message in error, you are not authorized to copy, distribute, or otherwise use this message or its attachments. Please notify the sender immediately by return e-mail and permanently delete this message and any attachments. Gartner makes no warranty that this e-mail is error or virus free.

From: Aronson, Lauren (CMS/OL) <[REDACTED]>
Sent: Thursday, September 12, 2013 10:14 AM
To: Park, Todd; Trenkle, Tony (CMS/OIS)
Cc: Baitman, Frank (OS/ASA/OCIO); Fryer, Teresa M. (CMS/OIS); Mellor, Michael (CMS/OIS); Cook, Brian T. (CMS/OC)
Subject: RE: Comment from Gartner Analyst Christian Byrnes

Yup. We have Gary Cohen testifying before Energy & Commerce next week so we could potentially use this.

From: Park, Todd [mailto:[REDACTED]]
Sent: Thursday, September 12, 2013 10:13 AM
To: Trenkle, Tony (CMS/OIS)
Cc: Baitman, Frank (OS/ASA/OCIO); Fryer, Teresa M. (CMS/OIS); Mellor, Michael (CMS/OIS); Cook, Brian T. (CMS/OC); Aronson, Lauren (CMS/OL)
Subject: Re: Comment from Gartner Analyst Christian Byrnes

Tony, I think this is super-helpful -- Brian and Lauren, perhaps this is something you can hold in reserve in case you need it?

From: Trenkle, Tony (CMS/OIS) [mailto:[REDACTED]]
Sent: Thursday, September 12, 2013 08:49 AM
To: Park, Todd
Cc: Baitman, Frank (OS/ASA/OCIO) <[REDACTED]>; Fryer, Teresa M. (CMS/OIS) <[REDACTED]>; Mellor, Michael (CMS/OIS) <[REDACTED]>
Subject: FW: Comment from Gartner Analyst Christian Byrnes

Todd,

Does this help?

Tony

From: Russell, DeLaine [mailto:[REDACTED]]
Sent: Wednesday, September 11, 2013 12:04 PM
To: Trenkle, Tony (CMS/OIS)
Cc: Heiliger, Christopher
Subject: Comment from Gartner Analyst Christian Byrnes

Tony,
Below is what I just received from the analyst. I hope this is what you are looking for. Chris is our most knowledgeable and experienced information security analyst.
Best,
DeLaine

Gartner Inc advises thousands of enterprise and government clients on best practices associated with the use of information technology. As a leader of the information security practice within Gartner Research I certify that the

From: Snyder, Michelle (CMS/OA) <[REDACTED]>
Sent: Thursday, October 10, 2013 5:03 PM
To: Park, Todd
Subject: FW: Item

A.Michelle Snyder
Chief Operating Officer
DHHS/CMS/OA
[REDACTED]

From: Trenkle, Tony (CMS/OIS)
Sent: Thursday, October 10, 2013 4:54 PM
To: Snyder, Michelle (CMS/OA); Tavenner, Marilyn (CMS/OA); Kerr, James T. (CMS/CMHPO)
Subject: RE: Item

Here's the answer below, maybe more detail than you want.

From: Schankweiler, Thomas W. (CMS/OIS)
Sent: Thursday, October 10, 2013 2:08 PM
To: Fryer, Teresa M. (CMS/OIS)
Cc: Ashbaugh, Jason L. (CMS/OIS); Linares, George E. (CMS/OIS); Outerbridge, Monique (CMS/OIS); Oh, Mark U. (CMS/OIS); Chao, Henry (CMS/OIS); Warren, Kevin (CMS/OIS)
Subject: RE: Admin passwords and insecurity in healthcare.gov

Hello all,

Here is the feedback regarding this inquiry.

Statement:

CMS (CIISG) acknowledges the feedback by the security community. Analysis of the code and a review of the operational environment has confirmed that the site is secure and operating with low risk to consumers.

The code that has been reposted to Pastebin and commented on by TrustedSec is intended to be available to the public code as it makes the user interface (UI) of the site function. By design, these "resource bundles" contain all of the non-personalized text the user will see throughout the site. There is no admin level ID's or passwords located within the java script posted on-line. The code base at CGI has also just been queried for strings such as "admin password" and "abc123gov" per the twitter screenshot. No evidence was located that there is admin credential revealed. The person who retweeted with the abc password is just being humorous.

The XOC Security team and the SCA test team does run all of the tools mentioned in the article. A lot of commented code was removed prior to production, and the need to perform JS comment-removal/minification/obfuscation is a roadmap item, in fact it is scheduled for release to the Test2 environment tonight. Performing minification requires a lot of testing to ensure the application is not broken during YUI compression. As java scripts can be improved they will be release with subsequent builds.

To the other points in the article The marketplace does not use PHP so that is a non-issue. The use of Captcha was considered at one time, but removed to ensure 508-Compliance and to more importantly to remove burden on a

consumer as *A Good Consumer Experience* was a design consideration. Also the concept of guessing ID's to see if there is a valid one or not is a known risk. We can look into taking steps at locking down access controls further, but it would negatively effect the user-experience.

Regards,

Tom Schankweiler, CISSP
Information Security Officer, CCIIO
CMS\OIS\CIISG
Consumer Information and Insurance Systems Group
[REDACTED] (Balt. Office, N2-13-22)
[REDACTED] (Mobile)

From: Snyder, Michelle (CMS/OA)
Sent: Thursday, October 10, 2013 4:41 PM
To: Trenkle, Tony (CMS/OIS)
Subject: Fw: Item

Could you take a look?

Sent from my BlackBerry Wireless Device

From: Tavenner, Marilyn (CMS/OA)
Sent: Thursday, October 10, 2013 04:10 PM
To: Snyder, Michelle (CMS/OA); Kerr, James T. (CMS/CMHPO)
Subject: FW: Item

Wanted you to have this in case you want to have tony reach out to them

From: Park, Todd [mailto:[REDACTED]]
Sent: Thursday, October 10, 2013 2:11 PM
To: Tavenner, Marilyn (CMS/OA)
Subject: Item

Marilyn, this got sent to me by someone who says these guys are on the level. I would suggest that the Marketplace IT security folks check it out (and potentially reach out to these guys as well)

https://www.trustedsec.com/october_2013/affordable_health_care_website_secure_probably/

Contact Us: 1.877.550.4728 | info@trustedsec.com



[Home](#) [Services](#) [Downloads](#) [Blog](#) [About Us](#) [Contact Us](#) [Q](#)

Is the Affordable Health Care Website Secure? Probably not.

Home / October_2013 / Is the Affordable Health Care Website Secure?

Probably not.

[< Previous](#) [Next >](#)

Is the Affordable Health Care Website Secure? Probably not.

With the Affordable Health Care Act moving into full momentum – there are a lot of privacy and security concerns for any new major government program being implemented. It's no secret that the website, the infrastructure, and the staffing has been a challenge to get up in running in the appropriate timeframes. Coming purely from the security industry and seeing corporations, deadlines, and tight timeframes snag security objectives – there should be major concern on the implications this system has on what will become the largest database of Americans in recorded history.

The Affordable Health Care Act websites cost an estimated 634 million to develop. <http://www.digitaltrends.com/opinion/obamacare-healthcare-gov-website-cost/>. One would hope that there would be heavy security integration into the software development lifecycle and best practices followed in the most extreme circumstances. As you can imagine, the site is going to be a major target for hackers, other governments, and organized crime. There's a lot of money to be made right now in an untapped market that is fresh for the picking.

We decided to look around – please note that there was nothing malicious, no hacking, and nothing intrusive involved in this test in any regard. We simply browsed the website as a normal visitor without any type of attacks at all. Just by looking at information, you can determine the quality of the code, and whether simple best practices in security are being followed.

Below is in the "Log In" page and the "Forgot password" link. Note when you enter a username that is invalid, it returns quickly that the username is invalid.

https://www.healthcare.gov/marketplace/global/en_US/registration#forgotPassword

HealthCare.gov [Learn](#) [Get Insurance](#)

New to HealthCare.gov? [CREATE ACCOUNT](#)

Forgot password

All fields are required unless they're marked optional

! Your information contains 1 error

- What is your Marketplace username? Important: This is not a valid Username

Please give us the following information and we'll send you an email with instructions.

What is your Marketplace username?

i Important: This is not a valid Username

[CANCEL](#) [SEND EMAIL](#)

Note when you place a valid user:

https://www.healthcare.gov/marketplace/global/en_US/registration#forgotPassword

HealthCare.gov [Learn](#) [Get Insurance](#)

New to HealthCare.gov? [CREATE ACCOUNT](#)

Forgot password

All fields are required unless they're marked optional

Please give us the following information and we'll send you an email with instructions.

What is your Marketplace username?

[CANCEL](#) [SEND EMAIL](#)

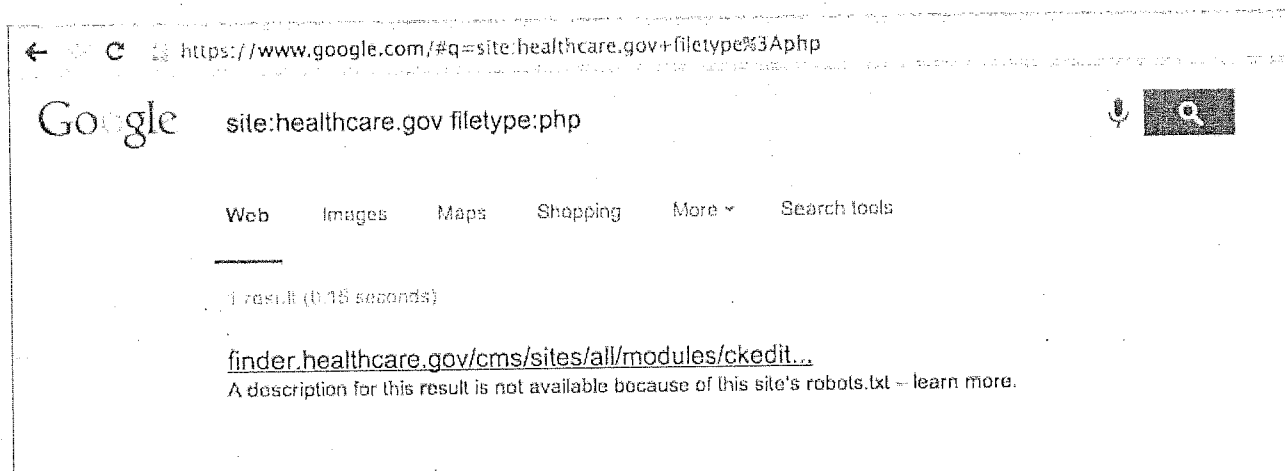
As you can see, you can enumerate valid and invalid user accounts in the database. Even worse is there are no form or appearance of automation deterrents such as CAPTCHA or image verifications that a human is attempting this. We can easily feed this through Burp Intruder for the content length from the response to see which usernames were

actually valid. Essentially you could enumerate the entire database of user accounts in the new healthcare.gov website through brute forcing the response codes and finding valid usernames.

Additionally, developer comment code is plastered everywhere which gives an attacker a significant amount of understanding about the application – these are literally everywhere on almost every page that's opened and all third party files:

```
//global variable used for SHOP upload functionality  
var myView = null;  
var agentBrokerSAMLToken=null;  
var postCCRApplclicantIDToken=null;  
var postCCRApplIDToken=null;  
var postCCRState=null;  
var agentEmailUUID =null;
```

Even crazier, doing some Google reconnaissance, we found an indexed site that a subsite used CKEditor – NOTE we did NOT attempt to even follow the link to verify if it's there.



CKEditor has a number of known exposures here: Search results for CKEditor on Exploit-DB

We've also identified some significant ones that we can't post online due to the critical nature of them and attempting to contact the development team for the website to remediate. Our intent is not to point out flaws, show flaws, or demonstrate insecurities, only to bring the light that based on viewing like a normal user, there appears to be things that would indicate that there should be major reason for concern here.

Again – nothing malicious performed here and we truly have no idea what the real exposures are without performing a full test on this, which we would have hoped would have been performed prior to any major production release.

By davek | October 9th, 2013 | October_2013 | Comments Off

Message

From: Park, Todd [REDACTED]
Sent: 6/26/2013 2:03:17 AM
To: Snyder, Michelle (CMS/OA) [/O=HHS EES/OU=First Administrative Group/cn=Recipients/cn=Michelle.Snyder.CMS];
Chao, Henry (CMS/OIS) [/O=HHS EES/OU=First Administrative Group/cn=Recipients/cn=Henry.Chao.OS]
Subject: RE: Draft writeup

Is it possible to get any edits/corrections/additional detail by COB Thursday?

Would love to loop back with Jeanne and Mark on Friday before I head out for (an attempted) vacation from July 1 to July 5. I gave Jeanne a heads up today to telegraph what's coming.

I think that the key will be to give Jeanne and Mark a bulletproof set of talking points they can use to push back in their conversations with the Blues and have the Blues truly understand why the logo play is a bad idea right now. (I don't think the Blues really understand that yet).

From: Snyder, Michelle (CMS/OA) [REDACTED]
Sent: Tuesday, June 25, 2013 5:48 PM
To: Park, Todd; Chao, Henry (CMS/OIS)
Subject: RE: Draft writeup

Looks good.....

A. Michelle Snyder
Deputy Chief Operating Officer
DHHS/CMS
[REDACTED]

From: Park, Todd [REDACTED]
Sent: Tuesday, June 25, 2013 1:13 AM
To: Chao, Henry (CMS/OIS); Snyder, Michelle (CMS/OA)
Subject: Draft writeup

Please keep close hold – loop in folks who can help with the details, but don't circulate broadly yet, if you don't mind. Let me know if this sounds right – any corrections/edits/additions/deletions welcome:

Attempting to integrate logos into the FFM for October 1 is not advisable. This is not because the act of integrating a logo is by itself a difficult thing to do. It's because the process for collecting health plan and product data from carriers via templates, loading these data into the HIOS system, validating the data, transferring the data from HIOS into the FFM QHP database, and having the rating engine retrieve and render that data in the FFM has been locked down, and is being utilized to support plan data collection/validation and system testing as we speak. Changing the underlying plan data template and processing routine right now -- by adding a new plan data element, the logo -- during the crunch-time sprint we're in from now to October 1, **would** introduce significant risk. Think of it as trying to change a gear in an airplane engine in mid-flight. Or adding a new field to an IRS tax form in the middle of filing season. As an isolated act, adding the field isn't hard. What's hard is the notion of adding it to the tax form via a system modification when that

system is going through an intense time, with a lot of moving parts involved, and where a wrong move could actually screw the whole system up.

An alternative to changing the core plan data submission/management process and systems (i.e., modifying the carrier plan data templates, HIOS, the QHP database, and rating engine logic) would be to set up a database of logos outside this core data management process and have the FFM system, when rendering a given insurance product, pull from both the QHP database plus the logo database. This is a terrible idea technically, would be prone to error, and still creates the issue of mucking with the jet engine while it's in flight.

The right way to add logos to the FFM would be to modify the core plan data submission/management process and systems to include logos as part of the carrier plan/product template and be able to process logos all the way through. This is not doable for Oct 1 without introducing significant operational risk to the go-live, as discussed above. We suggest considering it as part of a future release, post October 1 – understanding that it will have to compete with a lot of priorities. The reasonable thing to do would be to target making this modification in time for the next cycle of plan bids, in 2014.

From: Chao, Henry (CMS/OIS) <[REDACTED]>
Sent: Monday, July 22, 2013 10:45 PM
To: Park, Todd; Tavenner, Marilyn (CMS/OA); Khalid, Aryana C. (CMS/OA); Snyder, Michelle (CMS/OA)
Cc: Kerr, James T. (CMS/CMHPO); Bowen, Marianne (CMS/OA); Trenkle, Tony (CMS/OIS)
Subject: RE: BCBSA meeting; chatting tonight
Attachments: Chronological account of testing tasks and current status of Issuer testing 7-22-2013.docx

Importance: High

Please see attached paper that describes where we are currently with testing with Issuers and provides a chronology of tasks and attempts to address the issues (most which are not correct or inaccurate) Captured by M. Siegler in a meeting I presume with the BCBSA.

Dan Miller on my staff led the gathering of the facts for this paper and Dan has been what I call the "IT Ombudsman" for CMS and Issuer testing coordination. Dan, myself, and the rest of my staff are willing to do whatever it takes to get the issuers through testing and hope they will work as a community to elevate themselves to an improved operational readiness posture rather than spend time pointing to last month's challenges that have been overtaken by events. Their collective energies from Association coordination to marketing to legal to IT to operations should be singularly focused on doing what it takes to get to October 1st.

Thanks and please let me know if you need me to walk you through the descriptions.

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

From: Park, Todd [mailto:[REDACTED]]
Sent: Monday, July 22, 2013 7:33 PM
To: Chao, Henry (CMS/OIS); Tavenner, Marilyn (CMS/OA); Khalid, Aryana C. (CMS/OA); Snyder, Michelle (CMS/OA)
Subject: RE: BCBSA meeting; chatting tonight

Thanks so much, Henry and (echoing Marilyn), take the time you need, and get it to us whenever you can tonight.... Thanks so much again,
Todd

From: Chao, Henry (CMS/OIS) [mailto:[REDACTED]]
Sent: Monday, July 22, 2013 7:23 PM
To: Park, Todd; Tavenner, Marilyn (CMS/OA); Khalid, Aryana C. (CMS/OA); Snyder, Michelle (CMS/OA)
Subject: Re: BCBSA meeting; chatting tonight

We'll address in the write-up coming around 9pm.

Henry Chao

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

(Pri)
(Alt)
(BB)

From: Park, Todd [mailto:]
Sent: Monday, July 22, 2013 07:16 PM
To: Tavenner, Marilyn (CMS/OA); Khalid, Aryana C. (CMS/OA); Snyder, Michelle (CMS/OA); Chao, Henry (CMS/OIS)
Subject: RE: BCBSA meeting; chatting tonight

Hi Henry, just spoke with Marilyn if your writeup tonight could address each point in the Siegler email (including the point about subsidy eligibility and back-end app processing being fully on paper), that would be terrific. For convenience, have repasted the Siegler text below ☺ Thanks so very much again for doing this!

Siegler email: "The specifics I wrote down from the meeting are as follows. BCBS claimed: there was a 90% failure rate on the initial "handshake" tests with issuers and the FFM; as of Friday BCBS had not been able to establish "full connectivity" with the FFM; HHS had scheduled testing of enrollment file transfers to begin on July 15 but that was delayed one week and is set to begin today; BCBS presented HHS with 23 eligibility scenarios (eg: family coverage no subsidy, single coverage with subsidy, etc) it wanted to test with their plan data on the FFM system but that testing has been limited to 6 scenarios and has not yet begun; there are no plans to test the FFM SHOP marketplaces before Oct 1; they expect subsidy eligibility and back-end application processing to be fully on paper even if an applicant fills out the online application. They said this could potentially result in 30 -90 day delays between when an applicant fills out an application and when a plan is actually able to enroll the applicant in coverage with a subsidy reduced premium."

From: Tavenner, Marilyn (CMS/OA) [mailto:]
Sent: Monday, July 22, 2013 6:59 PM
To: Park, Todd; Khalid, Aryana C. (CMS/OA); Snyder, Michelle (CMS/OA); Chao, Henry (CMS/OIS)
Subject: Re: BCBSA meeting; chatting tonight

Todd please call me if you want to talk. [REDACTED]

From: Park, Todd [mailto:]
Sent: Monday, July 22, 2013 06:57 PM
To: Tavenner, Marilyn (CMS/OA); Khalid, Aryana C. (CMS/OA); Snyder, Michelle (CMS/OA); Chao, Henry (CMS/OIS)
Subject: RE: BCBSA meeting; chatting tonight

Apologies for the quick follow-on email would very much love to chat tonight for a few minutes; will make myself available any time; just name the time; thanks so much!

Todd

From: Park, Todd
Sent: Monday, July 22, 2013 6:51 PM
To: marilyn.tavenner; Khalid, Aryana C. (CMS/OA); michelle.snyder
henry.chao
Subject: FW: BCBSA meeting

Hi Marilyn, Aryana, Michelle, and Henry, hope you had a terrific weekend! I think you've already seen the email below, and you may already be writing up your thoughts on it.... In whatever way is most time-efficient for you (including jumping on the phone for a few minutes tonight, if that is easiest), was hoping to get your thoughts to be prepped for the ACA outreach meeting tomorrow morning at 11 (if this comes up as a topic of discussion) [REDACTED]

What might work best for you? Thanks so much,
Todd

From: Siegler, Matthew [mailto:[REDACTED]]
Sent: Monday, July 22, 2013 05:03 PM
To: Lambrew, Jeanne; Hash, Michael (HHS/OHR) <[REDACTED]>; Nelson, Karen <[REDACTED]>; Primus, Wendell <[REDACTED]>; David Schwartz <David.Schwartz@hhs.gov>; Aronson, Lauren (CMS/OL) <[REDACTED]>; Egorin, Melanie <[REDACTED]>; Miller, Erin <[REDACTED]>
Subject: BCBSA meeting

Hi All,

Sorry for the memory lapse, but the paper BCBS left with us did not go into specifics on the testing/readiness issues. They said they would send us that information. I've just pinged them about it and will share as soon as we have.

The specifics I wrote down from the meeting are as follows. BCBS claimed: there was a 90% failure rate on the initial "handshake" tests with issuers and the FFM; as of Friday BCBS had not been able to establish "full connectivity" with the FFM; HHS had scheduled testing of enrollment file transfers to begin on July 15 but that was delayed one week and is set to begin today; BCBS presented HHS with 23 eligibility scenarios (eg: family coverage no subsidy, single coverage with subsidy, etc) it wanted to test with their plan data on the FFM system but that testing has been limited to 6 scenarios and has not yet begun; there are no plans to test the FFM SHOP marketplaces before Oct 1; they expect subsidy eligibility and back-end application processing to be fully on paper even if an applicant fills out the online application. They said this could potentially result in 30-90 day delays between when an applicant fills out an application and when a plan is actually able to enroll the applicant in coverage with a subsidy reduced premium.

Thanks,

Matt

Matthew Siegler
Counsel
Committee on Energy and Commerce
Subcommittee on Health
Democratic Staff
[REDACTED]

Per our discussion and forwarded email from M. Siegler, here are key facts about the current state of engaging the issuers testing the enrollment functions of the FFM and Data Services Hub. My team and I believe that the first few bullets should illustrate the chronology of testing events/tasks since the end of May when the Trade Associations welcomed our revised accelerated testing approach. The last few bullet points attempts to objectively address the key issues raised by the BCBSA.

- **Acceleration of Issuer Testing Engagement Since End of May**: At the end of May, CMS announced to the issuer community a greatly accelerated FFM & Data Service Hub testing schedule, in which the key activities of issuer onboarding, connectivity testing with the Data Services Hub, issuer-initiated Direct Enrollment and FFM-initiated Enrollment transaction testing (834), and Plan Preview testing would launch with a series of thrice-weekly technical webinars in June and July, rather than waiting for those activities to occur in mid-to-late August as had been previously communicated. The Trades expressed their gratitude at the acceleration; AHIP called Aryana Khalid on May 21st after Henry announced the acceleration on May 17th to thank CMS and to say they knew what a heavy lift it was to move testing up.
- **Thrice-Weekly Issuer Technical Webinars**: Since May 30th, CMS has held 20 webinars and interactive Q&A sessions to engage issuers in the onboarding and issuer enrollment integration testing process, including the creation of the “CMS-Issuer Testing Technical Work Group” and “CMS-Issuer EDI Technical Work Group” webinars regularly attended by 200-300 participants per session, and each including Q&A between issuers and CMS’s technical subject matter experts.
- **CMSzONE and CMS Technical Document Dissemination to Issuers**: Since May 30th, CMS has posted 58 technical guidance documents on CMSzONE, a secure, online repository for the issuer testing community, including the Issuer Onboarding Guide & Testing Handbook, Direct Enrollment Test Data documentation and EDI Test Files, onboarding instructions, issuer testing frequently asked questions (FAQ’s) and all documents shared during the technical webinars.
- **Issuer Onboarding & Testing Steps**: In order for an issuer to conduct end-to-end testing they must accomplish three key activities:
 1. Complete an onboarding form that identifies how their respective system will connect with the Data Services Hub
 2. Complete configuration of electronic file transfer (EFT) in the pushing or pulling of enrollment transaction files (EDI 834 transactions for example)
 3. Complete Web connectivity testing for those issuers participating in Direct Enrollment.

Of those three key activities, the following bullet points indicate where we currently stand and hopefully clarifies some of the issues that in some cases are non-issues:

- **Issuer Onboarding Status**: 143 issuers have submitted onboarding forms to date; however, of the issuers who have submitted QHP’s directly in the HIOS system for the 19 FFM States, as of the end of last week, CMS is still waiting to hear from more than 60 issuers organizations who have not yet submitted a form at all the first step in the onboarding process that CMS launched in mid-June.
- **Most Issuers were not ready as of 7/15**: Based on our close monitoring of progress by Issuers, CMS made an announcement during the week before leading up to 7/15 start of testing, because of low percentage of Issuers that have been able to complete connectivity testing (less than 10 Issuers out of 75 Issuers having completed connectivity testing before 7/15), CMS decided to extend the Connectivity testing until 7/19 and provide additional/focused technical assistance during the week of 7/15. From that effort, we’ve more than doubled the number of Issuers that are now ready for Integrated testing with FFM.
- **Issuer EFT Connectivity Status**: Of the 143 issuers who have submitted onboarding forms, 63 issuers have completed EFT configuration for the outbound and inbound receipt of 834 files; CMS is waiting on some information from 35 issuers in order to complete this step (and an additional 9 issuers who were just added via the onboarding process). When initially establishing connectivity with the issuers in early July, technical configuration issues were discovered on both the CMS and the issuer sides. In order to optimize the remaining testing time, and to avoid the time involved in individual configuration and troubleshooting, on July 18th, CMS began switching many issuers from a “push” to a simpler “pull” model in order to complete connectivity.

- **Issuer Web Services (Direct Enrollment) Connectivity Status :** Of the 75 issuers participating in Direct Enrollment, CMS is still waiting on 38 issuers who have not yet responded in supplying the required information to start the Web Services test. Of the remaining 37 issuers, all have been set up by CMS, and of those, 24 issuers have passed the Web Services connectivity testing.
- **SHOP Testing:** CMS has focused issuer testing first and foremost on individual Direct Enrollment and Enrollment to 834 Transaction (834 is the HIPAA Standard Transaction for Health Plan Enrollment) testing as it relates to the individual marketplace, as this covers the broadest and most complex functionality in advance of October 1st. CMS has placed SHOP testing (as well as other aspects such as Lead Generation Testing) as a secondary priority once the former is underway. CMS does anticipate testing SHOP with the issuers in advance of October, and plans to hold a SHOP testing-specific webinar in order to launch SHOP variation of testing in mid-August. The SHOP testing will in essence be a simpler version of individual marketplace testing, as it does not entail the complications associated with eligibility, verifications, APTC or CSR calculations.
- **Scenarios:** CMS is making more than 23 direct enrollment scenarios part of the Direct Enrollment integration testing, including all of the scenarios that BCBSA had proposed. For 834 scenarios, CMS limited the overall scope to ensure that all issuers would be able to accomplish the required functionality during testing. Once all issuers are able to complete issuer enrollment integration testing, CMS plans to expand the number scenarios.
- **Enrollment File Transfers Testing :** After initial plans to begin testing of enrollment file transfers on July 15th, CMS began sending out the first 834 enrollment files to issuers on Friday, July 19th and has continued testing with the "Wave 1" issuers during the week of July 22nd.
- **Testing Dependency on State DOI Transfer of QHP's in Partnership States:** There are dependencies upon State DOI's to proceed in testing for those issuers in Partnership (SPM's) states and State Based Marketplaces (SBM's), because issuers can only test against those QHP's once they are transferred by the State DOI from NAIC's SERFF system to CMS's FFM system. The State DOI's have until July 31st to transfer the QHP's; until the QHP's for any given Partnership or NAIC State are transferred, only issuers with QHP's in one of the 19 FFM HIOS States will be able to participate in enrollment/834 testing with their QHP data.
- **Application Online Processing:** BCBSA mentions there are back end delays that could be 30 -90 days but they must have something mistaken or the thought was incorrectly captured because applicants that fill out the online application are not required to have the paper application filled out; their enrollments can be processed in a very short timeframe (e.g. 20 -40 minutes.)

From: Lambrew, Jeanne
Sent: Tuesday, July 23, 2013 9:38 AM
To: Tavenner, Marilyn (CMS/OA); Park, Todd
Cc: Khalid, Aryana C. (CMS/OA); Hash, Michael (HHS/OHR)
Subject: RE: Issuers

What do we do about the 25 Hill staffers who heard this information yesterday / many more who may still continue to be hearing this from the Blues through briefings?

From: Tavenner, Marilyn (CMS/OA) [mailto:]
Sent: Tuesday, July 23, 2013 9:34 AM
To: Lambrew, Jeanne; Park, Todd
Cc: Khalid, Aryana C. (CMS/OA); Hash, Michael (HHS/OHR)
Subject: Issuers

We have heard again from AHIP that the "issues" are with the Blues.....and I am going to have both the Blues and AHIP in tomorrow with Henry et al and see if I can figure it out and make clear how we move forward. I would appreciate being able to do that first.....and would ask for your support. Thanks Marilyn

From: Park, Todd
Sent: Tuesday, July 23, 2013 9:40 AM
To: Tavenner, Marilyn (CMS/OA); Lambrew, Jeanne; Khalid, Aryana C. (CMS/OA)
Cc: Cavanaugh, Alicia A. (CMS/OA); Miller, Ruth A. (CMS/OA)
Subject: RE: Touch base on issuers

Just finished talking with Henry and team. Have additional content clarification, and also a clear sense of what we need to tell BCBSA in terms of how we all need to work together constructively going forward -- Marilyn, I think this would be useful info for you going into your meetings tomorrow with BCBSA and AHIP. I have to give brief remarks at an event at 10 am (for which I need to prepare now), but can talk at 10:30 am, or anytime between 12 and 3. Thoughts?

-----Original Message-----

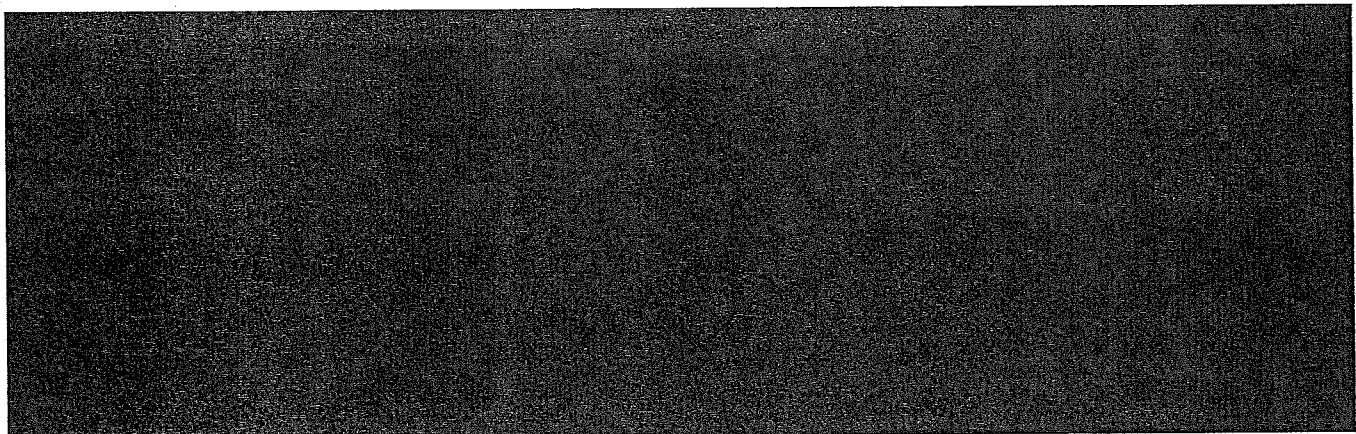
From: Tavenner, Marilyn (CMS/OA) [mailto:████████████████████]
Sent: Tuesday, July 23, 2013 8:48 AM
To: Park, Todd; Lambrew, Jeanne; Khalid, Aryana C. (CMS/OA)
Cc: Cavanaugh, Alicia A. (CMS/OA); Miller, Ruth A. (CMS/OA)
Subject: Touch base on issuers

Can we try for a conference call this am. Among us to discuss issues. Thanks.

From: Tavenner, Marilyn (CMS/OA) <[REDACTED]>
Sent: Tuesday, July 23, 2013 8:43 PM
To: Park, Todd; Chao, Henry (CMS/OIS); Snyder, Michelle (CMS/OA)
Subject: Re: Meeting today

Todd gave a great description of the meeting today. [REDACTED] Having Todd in our camp and knowledgeable is very very helpful!!

From: Park, Todd [mailto:[REDACTED]]
Sent: Tuesday, July 23, 2013 08:18 PM
To: Chao, Henry (CMS/OIS); Snyder, Michelle (CMS/OA)
Cc: Tavenner, Marilyn (CMS/OA)
Subject: Meeting today



On another front, close hold, as a result of the fire drill last night/this morning, and conversations that have been had with BCBSA/AHIP in its aftermath, it looks like substantial improvements will happen in terms of the dynamic on that front. Marilyn will discuss with you in more detail. So hopefully that fire drill was not in vain.

Massive, massive, massive gratitude again for everything that Team CMS has done and continues to do. May the Force continue to be with you, and God bless you,

Todd