LAMAR S. SMITH, Texas
CHAIRMAN

EDDIE BERNICE JOHNSON, Texas
RANKING MEMBER

Congress of the United States
House of Representatives

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

2321 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515–6301

(202) 225–6371
www.science.house.gov

MEMORANDUM

TO: Members and Staff of the Science, Space, and Technology Subcommittee on Oversight
FROM: Oversight Subcommittee Staff
DATE: September 12, 2014
RE: Science, Space, and Technology Subcommittee on Oversight Business Meeting

The Science, Space, and Technology Subcommittee on Oversight will meet on **Wednesday, September 17, 2014, at 4:00 p.m.** in **Room 2325** of the Rayburn House Office Building to consider the following:

- **Resolution Authorizing the Issuance of Subpoenas**

Purpose

The resolution authorizes the issuance of a subpoena *ad testificandum* to Todd Park former Chief Technology Officer of the United States, Office of Science and Technology Policy (OSTP), for his appearance before the Subcommittee on Oversight and a subpoena *duces tecum*, for any and all written or electronic communications, information, documents, and other records of Todd Park, during his tenure as Chief Technology Officer of the United States, relating to the HealthCare.gov website.

Background

On October 1, 2013, under the provisions of the Patient Protection and Affordable Care Act (ACA), the Administration launched HealthCare.gov, a federally-operated health insurance exchange website to help uninsured people find health care coverage.

The data passing through the HealthCare.gov website is one of the largest collections of personal information ever assembled, linking information from seven different federal agencies along with state agencies and government contractors. When launched last year, users attempting to gain information on potential healthcare coverage through the website were required to input personal contact information, birth dates and social security numbers for all family members, as well as household salary, among other data.

November 2013 Hearing

The House Science, Space, and Technology Committee (SST or Committee) oversees the agencies responsible for setting cyber privacy and security policies and standards for the rest of the federal government - the White House Office of Science and Technology Policy and the National Institute for Standards and Technology (NIST).

When the site was launched on October 1, 2013, it was plagued with operational problems. In light of the myriad of problems facing the website, on November 19, 2013, the Committee held a hearing to explore the threat posed by identity theft to Americans if hackers acquired such information through the HealthCare.gov website.[1] The hearing also examined issues related to the website's security controls and potential vulnerabilities by inviting cybersecurity experts to discuss what specific security standards and technical measures should be in place to protect Americans' privacy and personal information on HealthCare.gov.

Federal agencies have an obligation to ensure that these private records have sufficient protection from misuse and security breaches under the Federal Information Security Management Act (FISMA). However, according to documents from the Department of Health and Human Services (HHS), the security of the healthcare website had not been fully tested when it was launched last year,[2] and cybersecurity experts at the November hearing expressed concern about flaws in the website that put the personal data of Americans using the website at risk to identity theft from cybercriminals/hackers.[3]

January 2014 Hearing

The Committee revisited these issues in a subsequent hearing on January 16, 2014,[4] which provided Members with an updated assessment of HealthCare.gov to determine the likelihood of personal information being accessed or compromised from an attack on the website. The hearing also examined the potential consequences of identity theft to Americans if hackers with malicious intent gained personal information through the website.

Congressional investigations into the flawed website have identified varying degrees of concern among those involved in developing the website prior to its launch last October. A Centers for Medicare and Medicaid Services (CMS) memo on the Federally Facilitated Marketplaces (FFM) System from September 3, 2013, noted that, "[t]here is the possibility that the FFM security controls are ineffective,"[5] and that "[i]neffective controls do not appropriately protect the confidentiality, integrity and availability

---

[1] SST hearing, "Is My Data on Healthcare.gov Secure?" November 19, 2013, available at: http://science.house.gov/hearing/full-committee-hearing-my-data-healthcaregov-secure.

[2] Robert Pear and Eric Lipton, "Health Website Official Tells of White House Briefings," The New York Times, November 13, 2013, available at: http://www.nytimes.com/2013/11/14/us/officials-say-they-dont-know-cost-of-health-website-fixes.html?_r=0.

[3] Matthew J. Belvedere, "No Security Ever Built Into Obamacare Site: Hacker," CNBC.com, November 25, 2013, available at: http://www.cnbc.com/id/101225308.

[4] SST hearing, "Healthcare.gov: Consequences of Stolen Identity," January 16, 2014, available at: http://science.house.gov/hearing/full-committee-hearing-healthcaregov-consequences-stolen-identity.

[5] CMS Memo, "Authorization Decision for the Federal Facilitated Marketplaces (FFM) System," available at: http://oversight.house.gov/wp-content/uploads/2013/11/9.3.13-Trenkle.pdf.

of data and present a risk to the CMS enterprise."[6] Later that month, a memo addressed to CMS Administrator Marilyn Tavenner stated, "From a security perspective, the aspects of the system that were not tested due to the ongoing development, exposed a level of uncertainty that can be deemed as a high risk for FFM."[7] Further, a senior security expert at CMS stated that she recommended against launching the HealthCare.gov website on October 1, 2013, because of "high risk security concerns."[8]

Todd Park

On October 31, 2013, the Committee sent the first letter to Mr. Todd Park, then-U.S. Chief Technology Officer (CTO),[9] requesting that he testify at a hearing on November 19, 2013, to address the Committee's concerns about the lack of privacy standards for personal information passing through the HealthCare.gov website and the threat posed to Americans if hackers on the Internet gained access to such information. Prior to his position as U.S. CTO, Mr. Park was the CTO at HHS, where he "led the successful execution of an array of breakthrough initiatives, including the creation of HealthCare.gov."[10]

As the U.S. CTO, Mr. Park sat in OSTP, and was considered part of OSTP leadership. As U.S. CTO, Mr. Park focused on "how technology policy and innovation can advance the future of our nation."[11] According to his biography, Mr. Park is "a highly accomplished health IT entrepreneur"[12] who together with Mr. Jeff Zients, "assembled and led the tech surge that overhauled HealthCare.gov, ultimately enabling millions of Americans to sign up for quality, affordable health insurance."[13]

In written testimony before the Committee on June 20, 2012, Dr. John Holdren, OSTP Director, explained that:

> "OSTP also supports me in my role as Assistant to the President for Science and Technology and the **U.S. Chief Technology Officer**, who sits in OSTP, in our functions advising the President on S&T dimensions of the policy challenges before the Nation, including strengthening the economy and creating jobs, **improving healthcare** and education, enhancing the quality of the environment, and advancing national and homeland security."[14]

---

[6] Ibid.

[7] Memo to Marilyn Tavenner from James Kerr and Henry Chao, "Federally Facilitated Marketplace – DECISION," September 27, 2013, available at: http://www.scribd.com/doc/180332001/CMS-Memo-on-Marketplace-Security.

[8] House Oversight and Government Reform Committee press release, "CMS Officials Launched Healthcare.gov Against Warning Agency's Top Cybersecurity Official," December 20, 2013, available at: http://oversight.house.gov/release/cms-officials-launched-healthcare-gov-warning-agencys-top-cybersecurity-official.

[9] Mr. Park resigned his position as U.S. CTO on August 29, 2014, per an e-mail from OSTP to the Committee.

[10] White House Blog, "Todd Park Named New U.S. Chief Technology Officer," March 9, 2012, available at: http://www.whitehouse.gov/blog/2012/03/09/todd-park-named-new-us-chief-technology-officer.

[11] OSTP website, Todd Park bio, available at: http://www.whitehouse.gov/administration/eop/ostp/about/leadershipstaff/park.

[12] Ibid.

[13] Ibid.

[14] SST hearing, "Examining the Priorities and Effectiveness of the Nation's Science Policies," June 20, 2012, available at: http://science.house.gov/hearing/full-committee-hearing-examining-priorities-and-effectiveness-nation%E2%80%99s-science-policies; [Emphasis added].

For these reasons, the Committee invited Mr. Park to testify before the Committee on five occasions:

- October 31, 2013, letter from Lamar Smith, Chairman, Science, Space, and Technology Committee, to Todd Park, U.S. Chief Technology Officer;
- November 13, 2013, letter from Lamar Smith, Chairman, Science, Space, and Technology Committee, to Todd Park, U.S. Chief Technology Officer;
- November 18, 2013, letter from Lamar Smith, Chairman, Science, Space, and Technology Committee, to John Holdren, Director, Office of Science and Technology Policy;
- March 27, 2014, letter from Lamar Smith, Chairman, Science, Space, and Technology Committee, to John Holdren, Director, Office of Science and Technology Policy;
- June 24, 2014, meeting between Lamar Smith, Chairman, Science, Space, and Technology Committee; Paul Broun, Chairman, Oversight Subcommittee of the Science, Space, and Technology Committee; Frank Wolf, Chairman, Appropriations Subcommittee on Commerce, Justice, Science, and Related Agencies; Chaka Fattah, Ranking Member, Appropriations Subcommittee on Commerce, Justice, Science, and Related Agencies; John Holdren, Director, Office of Science and Technology Policy; and Todd Park, U.S. Chief Technology Officer.

OSTP declined all the invitations, citing a variety of reasons:

- "OSTP has not been substantially involved in the privacy and security standards that are in place for healthcare.gov."[15]
- "[T]he Office of Science and Technology Policy (OSTP) has not been substantially involved in the privacy and security standards for healthcare.gov. Thus, neither Mr. Park nor any other OSTP staff member is in a position to testify on the data security standards of the website."[16]
- "[W]hen asked about the security features of the healthcare.gov website during a hearing yesterday before another committee, Mr. Park explained that he has not been working on these issues."[17]
- "Mr. Park and OSTP personnel have not been substantially involved in developing or implementing the Federally Facilitated Marketplace's (FFM) security measures. In attempting to arrive at an appropriate accommodation, this is worth emphasizing. Mr. Park is not a cybersecurity expert; he did not develop or approve the security measures in

[15] November 8, 2013, letter from Donna Pignatelli, Assistant Director for Legislative Affairs, Office of Science and Technology Policy, to Lamar Smith, Chairman, Science, Space, and Technology Committee.
[16] November 14, 2013, letter from Donna Pignatelli, Assistant Director for Legislative Affairs, Office of Science and Technology Policy, to Lamar Smith, Chairman, Science, Space, and Technology Committee.
[17] Ibid.

place to protect the website, and he does not manage those responsible for keeping the site safe."[18]

Further, in testimony before the Oversight and Government Reform Committee on November 13, 2013, in response to questions by Members of Congress, Mr. Park said:[19]

- "I don't actually have a really detailed knowledge base of what actually happened pre-October 1. I don't know what levers were available. So I would hesitate to make any point now."
- "I am not even familiar with the development and testing regimen that happened prior to October 1. So I can't really opine about that."
- "I am part of an all-hands-on-deck effort to mobilize across the Administration to actually help under Jeff Zients' leadership. And in the lead-up to October 1, that wasn't part of my role."

In its review of documents to ascertain the role of Todd Park relative to HealthCare.gov, the Committee has determined that Mr. Park was a White House co-chair of the Affordable Care Act Information Technology Exchanges Steering Committee (**Attachment 1**). The stated mission of this HealthCare.gov Steering Committee is to support the timely and efficient resolution of barriers to assure the implementation of "consumer-centric" health insurance exchanges. The Steering Committee's Charter explicitly directs the participants "to promote resolution to key IT strategy and policy issues that impede progress on Affordable Care Act activities across the federal government and with the state exchanges," and to "direct the formulation of work groups to identify barriers, develop or identify promising practices to support efficiencies, and develop option papers for the Committee's consideration." The ACA Exchanges Steering Committee oversees both security and privacy interagency working groups.

Further, by working with other House committees, the Science Committee received some e-mails that suggest Mr. Park did indeed have a detailed knowledge base of HealthCare.gov before October 1, 2013, and that he appeared to be involved in developing the security standards and public statements about the security of the website (**Attachment 2**).

These documents should have been provided to the Committee pursuant to a request in a letter addressed to Dr. Holdren on December 20, 2013,[20] in which he was asked to provide all records and information regarding the Affordable Care Act, HealthCare.gov, or the ACA IT Exchanges Steering Committee. In addition, the Committee requested all records and emails to or from any and all OSTP employees, including Mr. Todd Park, regarding the ACA, Healthcare.gov, or the ACA Information Technology Exchanges Steering Committee. The broad nature of the document request is further highlighted by the fact that the Committee requested

---

[18] July 3, 2014, letter from John Holdren, Director, Office of Science and Technology Policy, to Paul Broun, Chairman, Oversight Subcommittee.

[19] Transcript of Oversight and Government Reform Committee hearing, "Obamacare Implementation: The Rollout of Healthcare.gov," November 13, 2013, available at: http://oversight.house.gov/wp-content/uploads/2014/06/11-13-13-TRANSCRIPT-Obamacare-Implementation-The-Rollout-of-Healthcare.gov_.pdf.

[20] December 20, 2013, letter from Lamar Smith, Chairman, Science, Space, and Technology Committee, to John Holdren, Director, Office of Science and Technology Policy.

copies of all records provided in the past, as well as those expected to be provided in the future, by OSTP to other Congressional committees in response to any ACA or HealthCare.gov document requests. While OSTP provided the Committee some records, it is evident from other documents in this Committee's possession that were not provided to us by OSTP, that OSTP failed to comply fully with the Committee's request. This raises questions about the extent of documents that may not have been provided to this and other congressional committees with similar requests.

Canceled Briefing

In yet one more attempt to work with OSTP, the Committee scheduled a briefing for Wednesday, September 10, 2014, by Todd Park for Members of the Oversight Subcommittee. The briefing was offered by OSTP, yet less than 24 hours before the briefing was scheduled to occur, OSTP cancelled it when they were informed that it was to be transcribed. For the sixth time, the Committee was denied the chance to question Mr. Park regarding his role in HealthCare.gov.

Questions Remain about HealthCare.gov's Security

Despite an improved ability for Americans to log on and create accounts on HealthCare.gov in their search for healthcare plans since the flawed October 1st launch, it is unclear how much work has been done to address the privacy and security concerns raised in the Committee's hearings. According to news reports over the past few months, the Centers for Medicare and Medicaid Services "denied a request by The Associated Press under the Freedom of Information Act for documents about the kinds of security software and computer systems behind the federally funded HealthCare.gov."[21] And, earlier this month, we learned that a "hacker broke into part of the HealthCare.gov insurance enrollment website in July and uploaded malicious software."[22]

A successful security breach of HealthCare.gov would be devastating to the millions of Americans forced by Administration regulations to enroll in health insurance plans through the website. Without proper security measures in place, participants are vulnerable to hackers who might be able to access such personal information, leaving them to deal with the consequences that come along with identity theft.

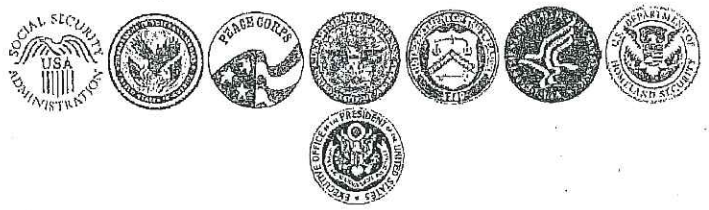
Chairman Broun seeks the Oversight Subcommittee's authorization to have subpoenas issued to Mr. Park in order to compel his records and his appearance before the Oversight Subcommittee to answer questions regarding the security of the website before the next open enrollment date.

There are a number of documents attached below that illustrate the points made in this memorandum and the need for further action on this matter.

---

[21] Jack Gillum, "US Won't Reveal Records on Health Website Security," Associated Press, August 21, 2014, available at: http://www.federalnewsradio.com/458/3684543/US-wont-reveal-records-on-health-website-security.

[22] Danny Yadron, "Hacker Breached HealthCare.gov Insurance Site," The Wall Street Journal, September 4, 2014, available at: http://online.wsj.com/articles/hacker-breached-healthcare-gov-insurance-site-1409861043.



Affordable Care Act IT Exchanges
Steering Committee
Charter

May 21, 2012

Project: Interagency Coordination for ACA IT Exchanges

TABLE OF CONTENTS

I. Purpose

This charter establishes the Affordable Care Act (ACA) IT Exchanges Steering Committee (Steering Committee) as a collaborative body and as a venue for seeking resolution of persistent interagency challenges and dependencies related to the implementation of IT exchanges in support of the Affordable Care Act.

This document outlines the mission, scope and responsibilities of the Steering Committee, identifies membership and support structures, and defines key processes and procedures. A Health Exchange Executive Secretariat (Executive Secretariat) has been established as an agent of the Committee to work with Agencies to ensure projects fully align under the Affordable Care Act in providing a streamlined and seamless interface with the America public and affected industries that will be impacted by the implementation of the health insurance exchanged under the Affordable Care Act.

II. Mission

The primary mission of the Steering Committee is to support the timely and efficient resolution of barriers while ensuring the realization of fully operational health insurance exchanges mandated under the Affordable Care Act. The Steering Committee will (a) address key Exchange information sharing policies and barriers, (b) work with Departments, Agencies, and other stakeholders as necessary on the implementation and execution of Health Insurance Exchanges.

III. Scope and Responsibilities

Steering Committee

The Steering Committee shall provide a forum for seeking resolution of interagency challenges and to further promote interagency alignments to assure the implementation of a consumer-centric health insurance exchanges under the Affordable Care Act. The Steering Committee can designate the Executive Secretariat to act on its behalf to meet these functions. The Steering Committee shall:

- Facilitate interagency discussions to promote resolution to key IT strategy and policy issues that impede progress on Affordable Care Act activities across the federal government and with the state exchanges
- Direct the formulation of work groups to identify barriers, develop or identify promising practices to support efficiencies, and develop option papers for the Committee's consideration.

- The Steering Committee will meet monthly or more frequently as deemed necessary by the Executive Secretariat, beginning in May 2012 through March 2014. The meeting frequency may be altered by the agreement of the Steering Committee Co-Chairs. Beginning in April 2014, the Steering Committee will meet on an *ad hoc* basis as advised by the Executive Secretariat or as requested by the Co-Chairs until it is the consensus of the Steering Committee members that the Exchange post-implementation issues have been sufficiently surfaced and addressed.

Executive Secretariat

The Executive Secretariat reports to the co-chairs and will support, coordinate, and act as a liaison between the Steering Committee and Departments.

The Executive Secretariat will remain operational through January 2015 or until it is the consensus of the Steering Committee members that the Exchange post-implementation issues have been sufficiently surfaced and addressed.

- Lead: HHS Program Management Office, Office of the Chief Information Officer
- Members: CMS, IRS, SSA

The Executive Secretariat's core functions will be as follows:

- Work with the designated workgroups to identify interagency IT policy issues for the Steering Committee's consideration
- Responsible for tracking and reporting progress of individual workgroups and elevating workgroup concerns to the Steering Committee.
- Share recommendation from the Steering Committee with workgroups and Agencies; distribute and support the implementation of these recommendations.
- Work closely with Agencies and stakeholders to develop and iterate the plans for resolution of challenges as appropriate.

Agencies will continue to coordinate ACA IT exchange project governance and oversight functions within their respective organizations and work directly with their IT project teams to ensure performance and alignment with the Steering Committee recommendations as appropriate.

Working Groups

Data Sharing and Privacy

- **Objectives:** Streamlining data use agreements and creating a uniform process for developing and maintaining computer matching agreements, data use agreements, ICAs, consent forms, etc..
- **Lead:** Janet Miner, IRS
- **Members:** HHS, SSA, DHS, VA, OPM, DoD, Peace Corps

Security Harmonization

- **Objectives:** Coordinate uniform process to harmonize security and streamline negotiations/documentation of new agreements within and across each agency
- **Co-Leads:** Tim May, SSA & Tom Schankweiler, CMS
- **Members:** HHS, IRS, VA, DHS, Peace Corps, OPM

Operational Oversight

- **Objective:** Provide a clearinghouse for issues needing to be analyzed and resolved among agencies for those issues not covered by other more specific workgroups, issue tracking and execution of common priorities in a timely/effective manner, and to assure the maximal alignment with the vision for a consumer-centric insurance exchange
- **Co-Leads:** Jim Kerr, CMS, Wanda Brown (IRS)
- **Members:** HHS, IRS, SSA, VA, DHS, Peace Corps, DoD, OPM

IV. Membership and Reporting Structure

The Federal Chief Information Officer (CIO), the Health Program Associate Director, and the U.S. Chief Technology Officer (CTO), in the Executive Office of the President will serve as co-Chairpersons for the Affordable Care Act IT Steering Committee. Membership will be comprised of senior executives from each of the participating Departments and Agencies who understand the ACA and health insurance exchange-related IT and business/mission needs of their Departments and Agencies and who can make key policy and management judgments on behalf of the respective Departments.

The following Departments and Agencies are represented on the Committee and will designate a senior executive as described above as members of the Steering Committee:

- Department of Health & Human Services, Centers for Medicare and Medicaid Services
- Department of Treasury, Internal Revenue Service
- Department of Homeland Security
- Department of Defense
- Department of Veterans Affairs

- Social Security Administration
- Peace Corps

Additional members may be added if additional interagency dependencies are identified.

Representatives from other Departments and offices, including subject matter experts (SMEs) and other advisors, may be invited to attend Steering Committee meetings with the concurrence of the Steering Committee co-Chairs.

V. Administration

A. Meetings

The Steering Committee shall meet as needed and as advised by the Executive Secretariat. Meetings may be in person, by conference call, or other "virtual" meeting tools. Materials shall be distributed to the members prior to the meeting in order for the members to have adequate time to review and consider the material. The members will be requested to review and provide comment/feedback on materials as appropriate.

B. Records Management

The Executive Secretariat will be responsible for appointing a designee to distribute materials prior to and post meetings (i.e., agenda, meeting minutes).

VI. Agreement

Steven VanRoekel, Executive Office of the President	Date
Keith Fontenot, Executive Office of the President	Date
Todd Park, Executive Office of the President	Date
Donna Roy, Department of Homeland Security	Date
Robert Carey, Department of Defense	Date
Frank Baitman, Department of Health & Human Services	Date
Marilyn Tavenner, HHS / Centers for Medicare & Medicaid Services	Date
Dorine Andrews, Peace Corps	Date

Bea Disman, Social Security Administration — Date

Terry Milholland, Department of Treasury/IRS — Date

Alan Constantian, Department of Veterans Affairs — Date

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@ostp.eop.gov' [Todd_Y_Park@ostp.eop.gov]; 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:Todd_Y_Park@ostp.eop.gov]
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

for this background and, more importantly, your great work to protect us from cyber attacks/security threats.

Chris

----- Original Message -----
From: Park, Todd
Sent: Tuesday, September 03, 2013 01:38 AM
To: Jennings, Christopher
Cc: Lambrew, Jeanne; Jones, Isabel; 'Aryana.Khalid@cms.hhs.gov' <Aryana.Khalid@cms.hhs.gov>; 'Michelle.Snyder@cms.hhs.gov' <Michelle.Snyder@cms.hhs.gov>; 'tony.trenkle@cms.hhs.gov' <tony.trenkle@cms.hhs.gov>; 'frank.baitman@hhs.gov' <frank.baitman@hhs.gov>; Graubard, Vivian
Subject: Re: Cybersecurity points

Hi Chris, here are an expanded/updated set of bullet points from Frank and Tony:

-- Like all publicly facing Internet websites, whether Amazon, Bank of America, or Medicare, we see regular attempts to infiltrate and test the security of our systems. We take these threats seriously, continuously monitoring for inappropriate activity, and adjusting our defenses accordingly.
-- The Centers for Medicare and Medicaid Services (CMS) has a history of preventing major breaches involving the loss of personally identifiable information from cyber-attacks. CMS faces unique challenges in maintaining a strong cyber security infrastructure because of its decentralized IT infrastructure and heavy dependence on contractors to perform most agency functions. To deal with these challenges, CMS has established an information security program with consistent risk management, security controls assessment, and security authorization processes for all enterprise systems. The security controls established and implemented by CMS meet existing Federal standards.
-- CMS has implemented a Security Operations Center (SOC) to provide additional monitoring capabilities and has been an innovative leader in using state of the art continuous monitoring tools. These tools can remotely scan the IT assets of CMS systems to ensure baseline configurations are up to date and compliant and that deviations are quickly identified and mitigated. Additionally these technologies have the capability to detect unknown or rogue hosts which are quickly identified and blocked. CMS has also implemented a penetration testing program to scan CMS systems to identify vulnerabilities and reduce or eliminate potential risks from external threats.
-- IT security for the Marketplace presents additional challenges because of short timelines, high visibility, multiple Federal and non-Federal partners, and new complex systems being built to support the program. CMS' information security staff have been working closely with IT development teams to help ensure that all required security testing is completed. Test results will then be reviewed by security staff: when the results are determined to be acceptable, an Authority to Operate (ATO) will be issued. The ATO is signed by both the CMS Chief Information Officer (CIO) and the Chief Information Security Officer (CISO).
-- CMS is working to ensure that all security testing is completed and ATOs are signed before October 1. A signed ATO signifies that the systems are operating at an acceptable level of risk and will meet tough Federal security standards. Once the Marketplace opens, CMS will utilize state of the art monitoring and surveillance tools to be able to quickly detect and deal with potential threats. CMS is also working closely with HHS and other public and private sector security experts to get additional technical support for the Marketplace program.
-- The U.S. standard for designing the information security program and responding to associated threats has been developed by the National Institute for Standards and Technology in support of the Federal Information Security Management Act. FISMA has emerged as the gold standard for information security standards and guidelines across the globe.
-- OMB has mandated the use of NIST standards for all federal civilian agencies, including HHS. HHS has developed a robust information security program across all of its operating divisions to ensure that the information security posture is robust and responsive to emerging threats. Working with the US-CERT at the Department of Homeland Security, HHS ensures that threats to information assets and networks are addressed and mitigated as rapidly as possible. This situational awareness and real-time mitigation activity embrace the newly launched systems in support of ACA through the coordination and collaboration mechanisms now in place at the Department.

----- Original Message -----
From: Jennings, Christopher
Sent: Monday, September 02, 2013 02:43 PM
To: Park, Todd
Cc: Lambrew, Jeanne; Jones, Isabel; 'Aryana.Khalid@cms.hhs.gov' <Aryana.Khalid@cms.hhs.gov>; 'Michelle.Snyder@cms.hhs.gov' <Michelle.Snyder@cms.hhs.gov>; 'tony.trenkle@cms.hhs.gov' <tony.trenkle@cms.hhs.gov>; 'frank.baitman@hhs.gov' <frank.baitman@hhs.gov>; Graubard, Vivian
Subject: RE: Cybersecurity points

Thanks Todd. And thanks Tony and Frank; would appreciate having as soon as is possible (with my preference, not surprisingly, being tonight before my stressful morning starts). Having said, guys, I will take what I can get when I get it with gratitude.

Chris

-----Original Message-----
From: Park, Todd
Sent: Monday, September 02, 2013 2:19 PM
To: Jennings, Christopher
Cc: Lambrew, Jeanne; Jones, Isabel; 'Aryana.Khalid@cms.hhs.gov'; 'Michelle.Snyder@cms.hhs.gov'; 'tony.trenkle@cms.hhs.gov'; 'frank.baitman@hhs.gov'; Graubard, Vivian
Subject: Re: Cybersecurity points

Hi Chris,

Tony and Frank will send you today an additional bullet point(s) regarding how the Federal Information Security Management Act (FISMA) and other legislation specific to Federal agencies has CMS and other agencies adhere to higher standards and go through a more rigorous level of assessment than is typical in the private sector.

Tony and Frank are also pulling together additional info on track record of defending against attacks, working with their info security people -- they are tracking folks down today and will seek to get you additional info by tonight.... But if it turns out they need until first thing tomorrow morning to get you the track record info, would that be OK?

Cheers,
Todd

----- Original Message -----
From: Jennings, Christopher
Sent: Monday, September 02, 2013 12:28 PM
To: Park, Todd
Cc: Lambrew, Jeanne; Jones, Isabel; 'Aryana.Khalid@cms.hhs.gov' <Aryana.Khalid@cms.hhs.gov>; 'Michelle.Snyder@cms.hhs.gov' <Michelle.Snyder@cms.hhs.gov>; 'tony.trenkle@cms.hhs.gov' <tony.trenkle@cms.hhs.gov>; 'frank.baitman@hhs.gov' <frank.baitman@hhs.gov>; Graubard, Vivian
Subject: RE: Cybersecurity points

Ok, thanks Todd. Quite helpful and will serve as placeholder [redacted] We need to have all of this locked down for September 11th hearing; we also have to have strong message with Justice, FTC, HHS and others for our enforcement event the week of the 16th. I know we had reference somewhere to current federal standards and how they exceed private sector as well as track record of protection from attacks. Can you or someone provide that reference for me to bolster confidence building tomorrow? Thanks much for all. And safe and fun travels my friend.

Chris

-----Original Message-----
From: Park, Todd
Sent: Monday, September 02, 2013 12:02 PM
To: Jennings, Christopher
Cc: Lambrew, Jeanne; Jones, Isabel; 'Aryana.Khalid@cms.hhs.gov'; 'Michelle.Snyder@cms.hhs.gov'; 'tony.trenkle@cms.hhs.gov'; 'frank.baitman@hhs.gov'; Graubard, Vivian
Subject: Cybersecurity points

Hi Chris, here are cybersecurity background points for you [redacted] The first three are the points CMS put together previously which I'm sure you've already seen; they are followed by a couple of points about next steps currently underway. Please let us know if you have any questions. I'll be on a long flight for much of Tuesday -- am looping Tony (CMS CIO), Frank Baitman (HHS CIO), Michelle, and Aryana, who can answer any questions you have that might arise.

-- The Centers for Medicare and Medicaid Services (CMS) has maintained a strong history of preventing major breaches involving the loss of personally identifiable information from cyber-attacks. CMS has in place established risk management, security controls assessment, and security authorization processes for all CMS systems. These controls meet or exceed existing Federal standards.

-- CMS has been an innovator leader in the information security community through the use of state of the art continuous monitoring tools that remotely scan the IT assets of CMS systems to ensure baseline configurations are up to date and compliant and that deviations are quickly identified and mitigated. Additionally these technologies have the capability to detect unknown or rogue hosts which are quickly identified and blocked. Penetration testing is also performed on all CMS systems to identify vulnerabilities and reduce or eliminate potential risks from external threats.

-- The IT systems that are being created for the Marketplace will meet or exceed existing Federal security standards and will utilize state of the art monitoring and surveillance tools. CMS is also

Message

From:	Park, Todd [Todd_Y_Park@ostp.eop.gov]
Sent:	9/2/2013 4:10:00 PM
To:	Trenkle, Tony (CMS/OIS) [/O=HHS EES/OU=First Administrative Group/cn=Recipients/cn=tony.trenkle.cms42098190]; Baitman, Frank (OS/ASA/OCIO) [/O=HHS EES/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=Frank.Baitman.OS]
CC:	Snyder, Michelle (CMS/OA) [/O=HHS EES/OU=First Administrative Group/cn=Recipients/cn=Michelle.Snyder.CMS]; Graubard, Vivian [Vivian_P_Graubard@ostp.eop.gov]; Mielke, Dawn M. [Dawn_M._Mielke@ostp.eop.gov]
Subject:	A couple of follow-ups

Hi Tony and Frank! A couple of follow-ups to my email to Chris below:

1. Just wanted to make sure that we're going to have DHS and DOJ folks on the 10 am call on Wed, as per our original plan?

2. It looks like the call with Alex Karp's top cyber folks will be 4 pm on Wednesday -- Tony, can you join this call? Feel free to have others join as well. Frank, I think you may be in a mtg, but if you can join as well, that would be terrific.... The agenda would be to (in confidence) discuss our cyber positioning and plans and get their thoughts. Dawn/Viv, can you make sure Tony/Frank are invited? Thanks!

Cheers,
Todd

----- Original Message -----
From: Park, Todd
Sent: Monday, September 02, 2013 12:02 PM
To: Jennings, Christopher
Cc: Lambrew, Jeanne; Jones, Isabel; 'Aryana.Khalid@cms.hhs.gov' <Aryana.Khalid@cms.hhs.gov>; 'Michelle.Snyder@cms.hhs.gov' <Michelle.Snyder@cms.hhs.gov>; 'tony.trenkle@cms.hhs.gov' <tony.trenkle@cms.hhs.gov>; 'frank.baitman@hhs.gov' <frank.baitman@hhs.gov>; Graubard, Vivian
Subject: Cybersecurity points

Hi Chris, here are cybersecurity background points for you [redacted] The first three are the points CMS put together previously which I'm sure you've already seen; they are followed by a couple of points about next steps currently underway. Please let us know if you have any questions. I'll be on a long flight for much of Tuesday -- am looping Tony (CMS CIO), Frank Baitman (HHS CIO), Michelle, and Aryana, who can answer any questions you have that might arise.

-- The Centers for Medicare and Medicaid Services (CMS) has maintained a strong history of preventing major breaches involving the loss of personally identifiable information from cyber-attacks. CMS has in place established risk management, security controls assessment, and security authorization processes for all CMS systems. These controls meet or exceed existing Federal standards.

-- CMS has been an innovator leader in the information security community through the use of state of the art continuous monitoring tools that remotely scan the IT assets of CMS systems to ensure baseline configurations are up to date and compliant and that deviations are quickly identified and mitigated. Additionally these technologies have the capability to detect unknown or rogue hosts which are quickly identified and blocked. Penetration testing is also performed on all CMS systems to identify vulnerabilities and reduce or eliminate potential risks from external threats.

-- The IT systems that are being created for the Marketplace will meet or exceed existing Federal security standards and will utilize state of the art monitoring and surveillance tools. CMS is also working closely with HHS and other public and private sector security experts to get additional technical support for the Marketplace program.

-- Tony Trenkle (CMS CIO) is convening a session next Wednesday, Sept 4, with CMS, HHS, DHS, DOJ, and me to review (1) our preparation for and defenses against cyberattack, (2) what our response/action would be in the event of an attack/crisis, and (3) how we would prosecute attackers. CMS will then produce a memo summarizing the above by the end of the week.

-- As an fyi, we have also reached out to Alex Karp and team. Alex put us in touch with his top cyber experts -- we are slated to speak with them on Wednesday as well.

Chris, again, please let us know if you have any questions!

All the best,

Message

From:	Park, Todd [Todd_Y_Park@ostp.eop.gov]
Sent:	8/29/2013 1:39:36 AM
To:	Trenkle, Tony (CMS/OIS) [/O=HHS EES/OU=First Administrative Group/cn=Recipients/cn=tony.trenkle.cms42098190]
CC:	Baitman, Frank (OS/ASA/OCIO) [/O=HHS EES/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=Frank.Baitman.OS]; Snyder, Michelle (CMS/OA) [/O=HHS EES/OU=First Administrative Group/cn=Recipients/cn=Michelle.Snyder.CMS]; Mielke, Dawn M. [Dawn_M._Mielke@ostp.eop.gov]; Graubard, Vivian [Vivian_P_Graubard@ostp.eop.gov]; Khalid, Aryana C. (CMS/OA) [/O=HHS EES/OU=First Administrative Group/cn=Recipients/cn=Aryana .Khalid .CMS]; Charest, Kevin (OS/ASA/OCIO/OIS) [/O=HHS EES/OU=First Administrative Group/cn=Recipients/cn=hel7]
Subject:	Re: Cyber next steps

Terrific, Tony, thanks, looking forward to it!

Todd

From: Trenkle, Tony (CMS/OIS) [mailto:tony.trenkle@cms.hhs.gov]
Sent: Wednesday, August 28, 2013 09:37 PM
To: Park, Todd
Cc: Baitman, Frank (OS/ASA/OCIO) <Frank.Baitman@hhs.gov>; Snyder, Michelle (CMS/OA) <Michelle.Snyder@cms.hhs.gov>; Mielke, Dawn M.; Graubard, Vivian; Khalid, Aryana C. (CMS/OA) <Aryana.Khalid@cms.hhs.gov>; Charest, Kevin (OS/ASA/OCIO/OIS) <Kevin.Charest@hhs.gov>
Subject: Re: Cyber next steps

I think that we all can agree on that. Todd, the call will follow the outline that you laid out in your email and our discussion should then drive what we say in the memo.

On Aug 28, 2013, at 7:38 PM, "Park, Todd" <Todd_Y_Park@ostp.eop.gov> wrote:
OK, will try to call in for a 10 am Wed meeting and make that work. And Frank, agree with your points about public-facing material.

Thanks!
Todd

From: Baitman, Frank (OS/ASA/OCIO) [mailto:Frank.Baitman@hhs.gov]
Sent: Wednesday, August 28, 2013 7:24 PM
To: Park, Todd; Trenkle, Tony (CMS/OIS)
Cc: Snyder, Michelle (CMS/OA); Mielke, Dawn M.; Graubard, Vivian; Khalid, Aryana C. (CMS/OA); Charest, Kevin (OS/ASA/OCIO/OIS)
Subject: Re: Cyber next steps

+ Adding Kevin

Todd et al,

Unfortunately the Secretary's Leadership Council is next Wed afternoon – and believe we'll have some IT items on the agenda, so I need to be there.

I believe we can address our defenses in a balanced manner: it should come as no surprise that we experience attacks and have defenses. But, for public facing material, we need to be careful to avoid too many details, and thereby avoid providing an instruction manual or worse, a challenge to malcontents to engage.

- Frank

From: <Park>, Todd <Todd_Y_Park@ostp.eop.gov>
Date: Wednesday, August 28, 2013 6:44 PM
To: "Trenkle, Tony (CMS/OIS)" <tony.trenkle@cms.hhs.gov>
Cc: "Snyder, Michelle (CMS/OA)" <Michelle.Snyder@cms.hhs.gov>, "Mielke, Dawn M." <Dawn_M._Mielke@ostp.eop.gov>, "Graubard, Vivian" <Vivian_P_Graubard@ostp.eop.gov>, Frank Baitman <frank.baitman@hhs.gov>, "Khalid, Aryana C. (CMS/OA)" <Aryana.Khalid@cms.hhs.gov>
Subject: RE: Cyber next steps

Tony, great, thank you, looping Aryana as well.

Might it be at all humanly possible to set up the meeting/call to happen between 1 and 4 pm on Wednesday? If that is not possible, I can try to figure something out, but just thought I'd check ☺

Aryana and I were also just in a meeting where we got some additional insight that is helpful:

- <!--[if !supportLists]--><!--[endif]-->There is a cyber and ACA subcommittee hearing happening on September 11, so it probably makes sense to target putting together a memo by end of next week (and talking with Alex Karp by end of next week to help inform the memo – will try to set up time with him for Thursday the 5th)
- <!--[if !supportLists]--><!--[endif]-->It sounds like folks would like the memo to cover (1) our preparation for and defenses against cyberattack, (2) what would our response/action be if an attack/crisis happened, and (3) how would we prosecute attackers. The roster for the meeting Michelle recommended (to include DHS and also DOJ to handle the prosecute part) sounds spot on.
- <!--[if !supportLists]--><!--[endif]-->Potentially for incorporation in the memo: external validators who could speak to the quality and strength of CMS cyberdefenses, should that become useful. Alex Karp could be one, but might you have others as well?

The memo is again for internal eyes only, but it sounds like people will draw from it in appropriate ways for external communications purposes as well.

Thanks!
Todd

From: Trenkle, Tony (CMS/OIS) [mailto:tony.trenkle@cms.hhs.gov]
Sent: Wednesday, August 28, 2013 5:44 PM
To: Park, Todd
Cc: Snyder, Michelle (CMS/OA); Mielke, Dawn M.; Graubard, Vivian; Baitman, Frank (OS/ASA/OCIO)
Subject: RE: Cyber next steps

Todd,

We are looking at setting up a call/meeting for next Wednesday morning at 10. I just spoke with Frank and that works for him. Teresa is already working with Kevin on pulling information together. I'll ask my scheduler to work with Dawn and Viv.

From: Park, Todd [mailto:Todd_Y_Park@ostp.eop.gov]
Sent: Wednesday, August 28, 2013 9:45 AM
To: Trenkle, Tony (CMS/OIS)
Cc: Snyder, Michelle (CMS/OA); Mielke, Dawn M.; Graubard, Vivian
Subject: Cyber next steps

Hi Tony, just spoke with Michelle, and she thinks our game plan makes sense, with additions:

1. <!--[if !supportLists]--><!--[endif]-->We should convene a work session in the next week with you, Teresa, Frank Baitman, his CISO, and probably a DHS person and DOJ person (she was thinking someone who has experience going after cyberattackers), plus any other folks you want to have there -- to discuss how to protect the Marketplace from cyberattack. This would include a discussion of our defenses, the threats, and our responses to the threats. I would absolutely love to be part of as much of this meeting as I can, but also don't want to be a scheduling bottleneck, and it should really happen sooner rather than later -- looping Dawn and Viv to help with my schedule. You should go ahead and schedule the meeting, and I will try to be there for as much of it as I possibly can!

2. <!--[if !supportLists]--><!--[endif]-->You/Teresa can then prepare a memo (could be for Michelle, for Marilyn, for others -- we'll figure that out) that basically outlines the protection strategy, including threat assessment and response strategy. This will be a memo that we pass on to WH leadership as well, fyi -- for internal use only.

3. <!--[if !supportLists]--><!--[endif]-->I will also reach out to Alex Karp today to let him know that we would love to speak with him about cyber and the Marketplace -- we should do a confidential, cone of silence consult with him after we've had our meeting as per item 1, not before; I'll set this up at the appropriate moment.

Does this sound cool to you?

Thanks!
Todd

Sent from my BlackBerry Wireless Device

---- Original Message ----
From: Park, Todd [mailto:Todd_Y_Park@ostp.eop.gov]
Sent: Tuesday, July 30, 2013 09:43 PM
To: Chao, Henry (CMS/OIS)
Cc: Snyder, Michelle (CMS/OA)
Subject: RE: Walk through of the online application in hc.gov

Hi Henry and Michelle, just circling back on the below, to see what general date range you think might make sense for this visit – would next week work? Just need to have a bit of advance time to line up Julian and David's schedules (and I'm out the week of August 12-16). Also: if you want to cut down on the time of the visit, ratcheting it down to something more like 60-90 minutes, or modify the agenda in any way, just let me know....

Thoughts? Thanks!
Todd

-----Original Message-----
From: Park, Todd
Sent: Thursday, July 25, 2013 3:01 PM
To: 'henry.chao@cms.hhs.gov'
Cc: 'Michelle.Snyder@cms.hhs.gov'
Subject: Re: Walk through of the online application in hc.gov

Hi Henry, thanks so much! To provide more context, as I shared with Michelle, I'll be bringing David Simas and Julian Harris (Keith Fontenot's successor, newly arrived) with me. Would love to (1) walk through the current live online workflow (ideally from the start of the application through Plan Compare and selection) and (2) provide the opportunity for Julian to get the latest update on (a) IT dev, (b) testing, and (c) operational prep.

For (2), Julian is interested in one level of detail below the POTUS presentation. I would not prepare any custom materials whatsoever for the meeting, but it would be great to show him (a) the slide you showed me with all of the IT modules/completion dates, (b) the testing summary for fed agencies, states, issuers you wrote up recently (I think for someone's testimony), or similar material, and (c) a slide (if you have it) of key operationalization steps (high level) on the road to Oct 1 and Dec 1 (e.g., contract X let, center X live, etc.).

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) [mailto:henry.chao@cms.hhs.gov]
Sent: Thursday, July 25, 2013 09:53 AM
To: Park, Todd
Cc: Oh, Mark U. (CMS/OIS) <mark.oh@cms.hhs.gov>; Couts, Todd (CMS/OIS) <Todd.Couts1@cms.hhs.gov>; Outerbridge, Monique (CMS/OIS) <monique.outerbridge@cms.hhs.gov>; Grothe, Kirk A. (CMS/OIS) <kirk.grothe@cms.hhs.gov>; Berkley, Katrina (CMS/OIS) <katrina.berkley@cms.hhs.gov>; Rhones, Rhonda D. (CMS/OIS) <Rhonda.Rhones@cms.hhs.gov>; Graubard, Vivian; 'rich.martin[redacted]<rich.martin[redacted]; 'cheryl.campbell[redacted]<cheryl.campbell[redacted]; 'Lakshmi.Manambedu[redacted]<Lakshmi.Manambedu[redacted]; 'Mark.Calem[redacted]<Mark.Calem[redacted]; 'Paul.Weiss[redacted]<Paul.Weiss[redacted]; Wallace, Mary H. (CMS/OC) <Mary.Wallace@cms.hhs.gov>; Booth, Jon G. (CMS/OC) <Jon.Booth@cms.hhs.gov>
Subject: Walk through of the online application in hc.gov

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.

Michelle mentioned you contacted her about this and that I should follow-up with you to schedule the walk through.

Katrina can work with Vivian to find a window of opportunity next week if you agree.

Let us know.

Thanks.

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

To: Couts, Todd (CMS/OIS) (Todd.Couts1@cms.hhs.gov)[Todd.Couts1@cms.hhs.gov]
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@cms.hhs.gov]
Sent: Friday, July 12, 2013 12:58 PM
To: Manambedu, Lakshmi (CGI Federal); Karlton Kim [redacted] Donohoe, Paul X. (CMS/OIS); Couts, Todd (CMS/OIS); Rhones, Rhonda D. (CMS/OIS)
Cc: Oh, Mark U. (CMS/OIS); Berkley, Katrina (CMS/OIS); Couts, 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

[redacted]

[redacted]

Appointment

From: Park, Todd [Todd_Y_Park@ostp.eop.gov]
Sent: 6/14/2013 2:59:12 PM
To: Park, Todd [Todd_Y_Park@ostp.eop.gov]; Snyder, Michelle (CMS/OA); Chao, Henry (CMS/OIS); VanRoekel, Steven; Lynch, Laura; Tran-Lam, Minh-Hai; Ple-Plakon, Alisa; Sivak, Bryan (HHS/IOS); Baitman, Frank (OS/ASA/OCIO); Kendall, Damaris (HHS/OS); Armstead, Andrea E. (CMS/OA); Seth, Sharman M. (CMS/OA); Reczek, Jeff; Overstreet, Tyler J.; Martin, Kathryn; Williams, Claudia; Schlosser, Lisa
Subject: Copy: ACA Sync-up
Location: [redacted]
Start: 6/26/2013 2:00:00 PM
End: 6/26/2013 3:00:00 PM
Show Time As: Busy

[redacted]

From: Park, Todd
Sent: Tuesday, June 11, 2013 07:52 PM
To: michelle.snyder@cms.hhs.gov <michelle.snyder@cms.hhs.gov>; henry.chao@cms.hhs.gov <henry.chao@cms.hhs.gov>
Cc: marilyn.tavenner@cms.hhs.gov <marilyn.tavenner@cms.hhs.gov>; VanRoekel, Steven; Graubard, Vivian; Lynch, Laura
Subject: Sync-up
Hi Michelle and Henry, hope all is terrific with you!

As you've heard from Marilyn, would love (with Steve) to arrange time (1 hour) in the next week or week and half to check in on how things are going with respect to Marketplace IT dev and testing. (And also to discuss the tactical question of issuer logos). Would love to arrange a visit to Baltimore, but given how crazy schedules are, I'm guessing that a videoconference or conference call would be more feasible.

We don't need any special documentation or whatnot. Just you ☺ If you have something that you've already put together for another purpose that you'd like to send, great.

May Vivian and Laura work with your office to set up a time to chat?

Cheers,
Todd

Message

From:	Khalid, Aryana C. (CMS/OA) [/O=HHS EES/OU=FIRST ADMINISTRATIVE GROUP/CN=RECIPIENTS/CN=ARYANA .KHALID .CMS]
Sent:	12/19/2012 6:10:13 PM
To:	Sivak, Bryan (HHS/IOS) [/O=HHS EES/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=Bryan.Sivak.os]; Snyder, Michelle (CMS/OA) [/O=HHS EES/OU=First Administrative Group/cn=Recipients/cn=Michelle.Snyder.CMS]
CC:	Chao, Henry (CMS/OIS) [/O=HHS EES/OU=First Administrative Group/cn=Recipients/cn=Henry.Chao.OS]; Claudia_H_Williams2@ostp.eop.gov; Cohen, Gary M. (CMS/CCIIO) [/O=HHS EES/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=Gary.Cohen1.CMS]; Mann, Cynthia (CMS/CMCS) [/O=HHS EES/OU=First Administrative Group/cn=Recipients/cn=Cynthia.Mann.CMS]; Todd_Y_Park@ostp.eop.gov; Vivian_P_Graubard@ostp.eop.gov; Kendall, Damaris (HHS/OS) [/O=HHS EES/OU=First Administrative Group/cn=Recipients/cn=damaris.kendall.os]; Trenkle, Tony (CMS/OIS) [/O=HHS EES/OU=First Administrative Group/cn=Recipients/cn=tony.trenkle.cms42098190]; Kerr, James T. (CMS/CMHPO) [/O=HHS EES/OU=First Administrative Group/cn=Recipients/cn=james.kerr.cms53763252]
Subject:	RE: Follow up on Consent/ID proofing

I hate to beat a dead horse, but I am going to. At this point we just need an answer. There is truly no point on having more and more circular conversations. Yesterday in my view was a disaster that seemed to just set us further back. I hope that we can get a solution today and hope that OMB and Todd can help get us there. I get that everyone on this email probably feels the same way.

Aryana

From: Sivak, Bryan (HHS/IOS)
Sent: Wednesday, December 19, 2012 1:05 PM
To: Snyder, Michelle (CMS/OA)
Cc: Chao, Henry (CMS/OIS); Claudia_H_Williams2@ostp.eop.gov; Cohen, Gary M. (CMS/CCIIO); Mann, Cynthia (CMS/CMCS); Khalid, Aryana C. (CMS/OA); Todd_Y_Park@ostp.eop.gov; Vivian_P_Graubard@ostp.eop.gov; Kendall, Damaris (HHS/OS); Trenkle, Tony (CMS/OIS); Kerr, James T. (CMS/CMHPO)
Subject: Re: Follow up on Consent/ID proofing

I agree with Henry and Michelle on this one. The goal is to walk out of the room with a solution today.

On Dec 19, 2012, at 12:49, "Snyder, Michelle (CMS/OA)" <Michelle.Snyder@cms.hhs.gov> wrote:
I must agree we are beyond this at this point

OMB OGC can decide the issue. We have provided an option that can happen. This needs to end - answer the threshold legal question and our ability to redisclose and move on - based on the decision we can make sure everyone understands the trade offs in terms of missing the October 1 date, costs, and consumer experience - quite frankly the risk of identity theft is the LEAST risky part of this entire enterprise.

Keith/Todd - can you help brink this to closure?

Michelle

Sent from my BlackBerry Wireless Device

From: Chao, Henry (CMS/OIS)
Sent: Wednesday, December 19, 2012 12:13 PM
To: Williams, Claudia <Claudia_H_Williams2@ostp.eop.gov>; Sivak, Bryan (HHS/IOS)
Cc: Park, Todd <Todd_Y_Park@ostp.eop.gov>; Graubard, Vivian <Vivian_P_Graubard@ostp.eop.gov>; Kendall, Damaris (HHS/OS); Trenkle, Tony (CMS/OIS); Kerr, James T. (CMS/CMHPO); Snyder, Michelle (CMS/OA)
Subject: RE: Follow up on Consent/ID proofing

Todd was present sat the ACA IT SC 3 weeks ago where I specified how to approach getting to the solution in time (which was needed 2 weeks ago) by having the key legal, policy, operations, IT, and a "chief mediator" of the process to drive to the strategic and tactical desired outcome of the administration.

No one heard me make this request and 3 weeks later you see the result of the meeting we had yesterday.

So with all due respect to you all, I do not agree with this approach and my intention is to walk in to the meeting at 4pm today and walk out with a decision. If we want to follow-up tomorrow to solidify the tactical execution steps then that's fine too, but I am again making a plea to take the approach suggested by the guy that has to lead a team to build this thing.

But as always I also know how to get in line when the formation command is sounded so if you want to go with the negotiated approach from last night, then so be it. You can count on my cooperation and support.

I sound this way only because we are seriously, seriously out of time and need to get to a decision for 2013/year one today.

From: Williams, Claudia [mailto:Claudia_H_Williams2@ostp.eop.gov]
Sent: Wednesday, December 19, 2012 12:00 PM
To: Chao, Henry (CMS/OIS); Sivak, Bryan (HHS/IOS)
Cc: Park, Todd; Graubard, Vivian; Kendall, Damaris (HHS/OS); Trenkle, Tony (CMS/OIS)
Subject: RE: Follow up on Consent/ID proofing

After meeting among EOP colleagues last night, we have decided to break the meetings into two segments.

1. Katie and Ellen will lead the first one working with HHS/SSA and IRS colleagues, which has the task of creating an identity proofing system that is operationally realistic and is as consumer driven as possible. So the conversation today is focused just on the ID proofing piece: what questions, what threshold

2. Todd and I hope to work with y'all on the second segment, focused on the IT Build (check box consent, enabling multiple accounts). That would be focus of our call tomorrow

Thanks, Claudia

From: Chao, Henry (CMS/OIS) [mailto:henry.chao@cms.hhs.gov]
Sent: Wednesday, December 19, 2012 11:50 AM
To: Williams, Claudia; Sivak, Bryan (HHS/IOS)
Cc: Park, Todd; Graubard, Vivian; Kendall, Damaris (HHS/OS); Trenkle, Tony (CMS/OIS)
Subject: RE: Follow up on Consent/ID proofing
Importance: High