

Mr. Todd Park, former Chief Technology Officer of the United States,
Office of Science and Technology Policy (OSTP)

RESPONSES TO QUESTIONS FOR THE RECORD
“The Role of the White House Chief Technology Officer
in the HealthCare.gov Website Debacle.”

U.S. House Committee on Science, Space, and Technology
Subcommittee on Oversight

Wednesday, November 19, 2014

Questions submitted by House Science, Space, and Technology Committee Chairman Lamar Smith and Oversight Subcommittee Chairman Paul Broun

1. **During the early construction and development of HealthCare.gov, including the Federally Funded Marketplace (FFM), were security issues ever raised, and if so, when were you made aware of them, by whom, and did you ever share those concerns with the President or anyone else at the White House?**
 - a. **Given the: (i) risks that were represented in the McKinsey report; (ii) risks that Michelle Snyder mentioned to you in the days leading up to the website; and (iii) the fact that CMS Administrator Marilyn Tavenner was going to make sure that the website launched on October 1, 2013, no matter what (Enclosure 1), at what stage in the development of the website and FFM was security fully implemented in compliance with federal standards?**

Response:

During the early construction and development of the Federally Facilitated Marketplace prior to its launch, I do not recall being made aware of particular problems with the security (i.e., the defenses against malicious cyberattack) of the Marketplace. My recollection of the McKinsey “red team” work in early 2013 was that it focused on how the project to develop the Federally Facilitated Marketplace was being executed in general, focusing on the development of the user-facing consumer experience, and how to improve the management of the project in this regard – as opposed to being focused on security. With respect to Michelle Snyder’s comments in the email chain to which I believe the question is referring, the thrust of that email chain was an effort to bring in additional hardware capacity to reinforce the Marketplace’s ability to support user load, rather than being a discussion about security. CMS is the best source of information regarding the security operations of the Marketplace, including when various certifications were issued in accordance with Federal requirements.

- 2. In your deep-dive sessions or status updates of HealthCare.gov, did anyone ever mention that an “end-to-end” test had been performed on the website? Were there ever any concerns about the website’s functionality and security during these meetings? If so, what was conveyed to you and what did you do with that information?**

Response:

In the particular sessions in which I participated prior to the launch of the Federally Facilitated Marketplace, I do not recall whether anyone mentioned that an end-to-end test had been performed. My recollection is that the McKinsey “red team” sessions in which I participated in early 2013 identified risks with respect to general project execution and the development of the user-facing consumer experience and recommended a series of actions to address these risks; this red team exercise did not focus on the cybersecurity defenses of the Marketplace. As discussed in my testimony, the red team’s analysis of project risks and recommended actions to address them were communicated to CMS, HHS, and White House senior leadership, and CMS agreed to adopt the key recommended actions, with the support of HHS and the White House. As with any large undertaking, I remember CMS from time to time explaining challenges they were working through to develop the Marketplace. In particular, I can recall specific open user-facing feature and functionality questions that were raised in discussions and that I worked to help resolve. As examples: I was asked by the White House Office of Health Reform to help assess whether it was feasible to add insurer logos to the display of insurance plans in the Marketplace; after talking with CMS about what such an effort would involve, the opinion I expressed to the Office of Health Reform was that it was not prudent to try to do so during this open enrollment season. I was also asked to assess CMS’s desire to push Spanish-language functionality to a post-October 1, 2013 deployment date; after talking with CMS, my assessment was that this made sense, which I conveyed to White House leadership. As discussed in my testimony, I was also asked by CMS to see if I could help facilitate getting additional hardware transported to the data center hosting the Marketplace in order to provide additional server capacity; I provided assistance as asked; CMS’s progress in this effort was tracked by CMS senior leadership and the White House Office of Health Reform; and my understanding from CMS was that the additional hardware was successfully transported to the data center and brought online.

- 3. Where was the quality control on the software development lifecycle and why did Americans see and experience so many issues during the initial rollout?**

Response:

In retrospect, the significant issues experienced by the Federally Facilitated Marketplace at launch reflect fundamental issues with how the Federal Government develops and deploys digital services – issues that have built up over decades and which have resulted in too many government digital service projects performing sub-optimally or worse. It is of vital importance that the Federal Government continue to accelerate efforts to (a) bring more of the best technology talent into government, revamping how we recruit, hire, and train personnel involved in all aspects of the development and operation of digital services for the public; (b) help attract more of the best companies into working with government, companies with strong

competency in modern digital service development approaches and techniques, which have been too often discouraged from competing for government contracts due to the complexity and archaic nature of traditional government procurement practices; and (c) radically revamp the process via which the government develops digital services in accordance with private sector best practices, including the utilization of agile, iterative approaches to software development, best-practice product management techniques, and contracting and budgeting practices that support these.

4. **The following quote comes from your bio previously posted on the OSTP page:**

“In 2013, the President called on Park, a highly accomplished health IT entrepreneur, to help with the successful turnaround of HealthCare.gov. Park, teamed with 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.”

As part of the effort to improve functionality after the website’s launch, what specific steps did you take relative to the website’s security, including security of people’s personal information?

- a. **What tests did you run on the website to ensure the level of effectiveness of security on the website?**
- b. **Was there ever end-to-end or comprehensive testing done?**
- c. **Did you address what a September 2014 GAO report described as existing weaknesses “in the processes used for managing information security and privacy, as well as the technical implementation of IT security controls?”¹**

Response:

My role in the turnaround of HealthCare.gov and the Federally Facilitated Marketplace post October 1, 2013 focused on helping to reduce the amount of time the site was down, improve the site’s speed, improve its ability to handle high user volume, and improve user-facing functionality (defined as user-facing features and workflow). My work did not focus on the security of the website – which continued to be handled by a dedicated CMS security team; CMS is the best source of information regarding the security operations of the website.

5. **Given your expertise and your involvement with HealthCare.gov, were you surprised to learn that the website was successfully hacked this summer? Do you know or have you**

¹ “HealthCare.gov – Actions Needed to Address Weaknesses in Information Security and Privacy Controls,” GAO, September 16, 2014, available at: <http://www.gao.gov/products/GAO-14-730>. (Emphasis added).

been made aware of any other incidents where personally identifiable information (PII) may have been illegally obtained through HealthCare.gov?

Response:

As context, my knowledge of the incident to which the question refers is second-hand – CMS will have more direct information. As far as I am aware, no personally identifiable information was compromised in the incident. I am not aware of any incidents in which personally identifiable information has been illegally obtained through HealthCare.gov.

6. **As you may know, there is no obligation on the federal government to disclose if Americans' sensitive personal information were breached in a cyber-attack. The House has passed legislation that requires HHS to notify people if their information is stolen from HealthCare.gov. As a former private businessman, HHS CTO and U.S. CTO, do you believe that the federal government should be required to inform Americans whenever their information is compromised from HealthCare.gov, and if so, how quickly?**

Response:

I haven't reviewed the legislation to which this question is referring. With respect to the legislation and this question in general, I would want to seek the opinions of sources such as OMB before forming my own views.

7. **At the November 19, 2014 hearing, you mentioned that you met with the President on at least two occasions regarding the status of HealthCare.gov. How many HealthCare.gov briefings did you actually participate in where the President was present?**
- a. **When was the first time you talked to the President about the security and privacy aspects of HealthCare.gov?**
 - b. **Did you ever discuss the operational readiness of HealthCare.gov with the President? If so, when, and what did you tell him about the website's security? Did you discuss any testing that had been done to ensure its readiness?**
 - c. **Was there ever a discussion about postponing the launch of the website? If so, did the President ever suggest a delay? Did you ever suggest to the President that he consider delaying the launch of the website?**

Response:

The two meetings on the implementation of the Affordable Care Act that included the President and senior White House leadership that I mentioned in my testimony at the hearing are the only two such meetings in which I can recall participating prior to the launch of the

Federally Facilitated Marketplace. In the first meeting, which was in April 2013, there were multiple presenters, and my role was to talk for approximately ten minutes and summarize the findings of the early 2013 McKinsey “red team” exercise – which identified general project execution and user-facing consumer experience risks and recommended a series of actions to address those risks and improve how the project was operating. In the second meeting, which was in July 2013, my role among the presenters was to discuss, for approximately ten minutes, follow-through on key red team recommendations (CMS agreed to adopt them all, with HHS and White House support) and CMS’s assessment of the current status of efforts to complete the intended functionality of the Marketplace. As I recall, the McKinsey red team exercise’s work did not focus on cybersecurity, and in neither meeting did my talk discuss the site’s cybersecurity defenses. With respect to postponing the launch of the website, I do not recall a discussion considering a delay of the launch of the website at either of those two meetings.

8. **At the Oversight and Government Reform hearing in November, 2013, Rep. Jim Jordan noted that according to White House logs, you attended nine White House meetings run by Ms. Jeanne Lambrew, to which you acknowledged attending meetings from “time to time”² on the subject of the Affordable Care Act. How many of these meetings included discussion of the ACA and HealthCare.gov website, and what was your role in the meetings?**

Response:

Prior to October 1, 2013, I was in meetings run by Jeanne Lambrew from time to time on the subject of the Affordable Care Act. To the best of my recollection, meeting topics included matters related to the development of particular regulations, outreach efforts, and Affordable Care Act implementation. I am not certain how many meetings specifically included discussion of HealthCare.gov and the Federally Facilitated Marketplace, but believe that a number of them did. My role in such meetings was generally to listen to presentations made by others and to offer thoughts and assistance in places where this would be helpful.

9. **Who did you most frequently meet with to discuss the Affordable Care Act and/or the HealthCare.gov website? Who at the White House did you most frequently meet with?**

Response:

Prior to October 1, 2013 (the time period to which I am assuming this question is referring), the people with whom I recall most frequently discussing the Affordable Care Act and/or the Federally Facilitated Marketplace were CMS management (including Michelle Snyder and Henry Chao), the White House Office of Health Reform (including Chris Jennings and Jeanne Lambrew), and the Office of Management and Budget (including Steve VanRoekel).

² “Obamacare Implementation – The Rollout of HealthCare.gov,” House Oversight and Government Reform Committee, 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](http://oversight.house.gov/wp-content/uploads/2014/06/11-13-13-TRANSCRIPT-Obamacare-Implementation-The-Rollout-of-HealthCare.gov.pdf). (Hereinafter OGR Transcript).

10. **Did you ever have a conversation about the operational readiness of HealthCare.gov with Dr. John Holdren, OSTP Director? If so, please describe in detail what was discussed?**

Response:

I do not recall having conversations with Dr. Holdren about the operational readiness of HealthCare.gov. I would let Dr. Holdren know from time to time when I was asked to spend time assisting with HealthCare.gov, but I do not recall briefing him in a substantive way about the content of this work.

11. **Referring to Enclosure 2 of this document, did the additional hardware from Verizon that you helped Mr. Chao order in the days leading up to the website launch perform as you expected?**
- a. **Who suggested that additional hardware was needed?**
 - b. **Is it typical to order and implement new hardware into a system hours before it is to be released to the public? If not, please explain the risks in doing so?**
 - c. **Were you concerned by the need to implement new hardware hours before the website launch? If not, why?**
 - d. **Why was the new hardware needed? Please describe the mistakes that lead to the need for this last minute fix.**
 - e. **Was the White House made aware of the issues that require this last minute fix? Who informed them?**

Response:

My understanding from CMS, which was the on-the-ground manager of what was happening, was that the additional hardware was successfully transported to the data center hosting the Marketplace and brought online. My recollection is that it was CMS's idea to seek to bring in additional hardware, to add capacity to the system. In my experience, it is not a rare occurrence to add server capacity on rapid timeframes to help increase system capacity. During the work to turn around and improve the Federally Facilitated Marketplace post October 1, 2013, our team added hardware and server capacity on rapid timeframes on multiple occasions – work that does need to be done with care and skill to ensure success. Based on my conversations with CMS management at the time, my understanding of why CMS moved to add more capacity prior to October 1 was due to the need to expand capacity given load testing results and in anticipation of high demand. As I recall, CMS made the White House (including me and the White House Office of Health Reform) aware of this effort. As previously discussed, CMS asked

me to help facilitate getting additional hardware transported to the data center hosting the Marketplace; I provided assistance as asked. CMS's progress in this effort was tracked by CMS senior leadership and the White House Office of Health Reform; my understanding from CMS was that the additional hardware was successfully transported to the data center and brought online.

12. **Referring to Enclosure 3, in the ACA Exchange IT Steering Committee meeting minutes, it notes that you were engaged in discussion on NIST Level 2 inter-mechanics. Who did you speak with and what was discussed?**

Response:

My recollection is that CMS asked OMB and me—as per the Steering Committee's mission to provide a neutral venue in which agencies could work through interagency items—to facilitate a conversation in which CMS, SSA, and IRS would discuss identity proofing. As part of my role as facilitator, via email and phone, I helped CMS connect with NIST resources (including a NIST employee then on detail to OSTP whom NIST asked to join the conversation), so that CMS could access their expertise on and knowledge of identity proofing and the meaning of NIST Level 2; I am not an expert on such matters. My recollection is that CMS, SSA, and IRS ultimately came to agreement on the topic of identity proofing themselves in a generally self-propelled way.

13. **Besides the ACA Exchange IT Steering Committee meetings, what other meetings did you attend where the HealthCare.gov website was discussed?**

Response:

In the period prior to October 1, 2013, in addition to the Steering Committee meetings, I attended a variety of meetings at CMS, HHS, and the White House which included discussion of HealthCare.gov and the Federally Facilitated Marketplace (on various aspects of implementation, consumer outreach, and presentation to consumers), including the meetings discussed in my answers to Questions 7 and 8. Other than as described in my answer to Question 7, my role in such meetings was generally to listen to presentations made by others and to offer thoughts and assistance in places where this would be helpful.

14. **In an email from Thursday, October 10, 2013, (Enclosure 4) you emailed Marilyn Tavenner an article from TrustedSec and stated, “this got sent to me by someone who says these guys are on the level.”**

a. Who sent you the TrustedSec article?

b. Did this person email you the article? If so, did they email it to your work or your personal email account?

Response:

On October 10, 2013, Bryan Sivak, the CTO of HHS, sent me the TrustedSec article – via email, to my work account. I sent it to CMS for evaluation. CMS responded shortly thereafter, saying that its analysis and review confirmed that “the site is secure and operating with low risk to consumers.”

As a note, in a subsequent conversation in an associated email, on a topic unrelated to the TrustedSec article, I stressed to the Administrator of CMS that it would be important for CMS to conduct thorough load testing and security testing of “Wave D,” which referred to new account management software functionality being developed by Marketplace contractor CGI that was potentially going to be deployed to help improve account management performance in the Federally Facilitated Marketplace. I was focused on this effort at the time (early October 2013) because by that time, I was engaged full-time in the HealthCare.gov turnaround effort, working night and day to help address issues, including the ability for users to create accounts and log on to the system; this is why I was writing to the Administrator of CMS on the topic. The new account management software functionality represented by “Wave D” was ultimately not deployed, as an alternate path to account management performance improvement (work dubbed “Wave C++” and subsequent activity pursued by Oracle and others) proved successful.

15. In your testimony before Congress in November 2013, you disagreed with Rep. Jim Jordan’s characterization of you as the “head of information technology for the entire United States,”³ stating that you are the “technology and innovation policy advisor in the Office of Science and Technology Policy.”⁴

While you were evidently part of OSTP leadership as CTO, and you state in your testimony that you joined “the White House Office of Science and Technology Policy as U.S. CTO,” OSTP Administrator John Holdren testified that you did not report to him in testimony he presented before the Committee earlier this year.

- a. What is the role of the U.S. Chief Technology Officer? If it has evolved over time, what changes in responsibilities have been made, and why?
- b. Who did you report to as U.S. CTO? Was the President technically your direct supervisor or was there someone else to whom you reported?
- c. Did you ever brief Dr. Holdren about HealthCare.gov? If so, at whose request, how often, and what did you convey to him?
- d. How did you distinguish between your responsibilities as advisor to the President and as leadership within OSTP? How did the OSTP staff who worked for you make that distinction?
- e. Was your salary as U.S. Chief Technology Officer paid through OSTP?
- f. Did anyone else at OSTP work on aspects of HealthCare.gov (including Presidential Innovation Fellows)? If so, who, and what did they work on?

Response:

My role as U.S. Chief Technology Officer was primarily to serve as an advisor across a broad portfolio of technology and innovation policy issues. I worked on open data policy and initiatives, wireless spectrum policy, how to advance a free and open internet, how to harness the power of technological innovation to fight human trafficking and improve disaster response and recovery, and more. My understanding is that my predecessor, Aneesh Chopra, the first U.S. CTO, also held the title of Associate Director for Technology, which carried with it the responsibility of overseeing Federal investment in technology research. When I assumed the role of U.S. CTO, unlike Mr. Chopra, I did not simultaneously take on the responsibilities of the Associate Director for Technology; this evolution was in order to enable me to devote the desired level of focus on technology and innovation policy. As to earlier conceptions of the U.S. CTO role, I cannot speak to those; I can speak to what I was asked to do in the role.

I was also an Assistant to the President. I took general direction from the White House Office of the Chief of Staff and specific direction from different individuals with whom I would work

³ Ibid.

⁴ Ibid.

on each of the technology and innovation initiatives in which I was involved.

I do not recall briefing Dr. Holdren about HealthCare.gov and the Federally Facilitated Marketplace in substantive ways. I would let Dr. Holdren know from time to time when I was asked to spend time assisting with HealthCare.gov, but do not recall briefing him in a substantive way about the content of this work.

As U.S. CTO and part of OSTP's leadership, I focused on technology and innovation policy, consistent with OSTP's mission. As an Assistant to the President, I held the same rank as Dr. Holdren, and therefore operated as his peer and as a partner, though Dr. Holdren holds overall management responsibility for the operations of OSTP.

OSTP paid my U.S. CTO salary.

With respect to others working in OSTP, other than as specified in my answer to Question 12, my recollection prior to October 2013 is that I would from time to time ask an HHS detailee to attend a HealthCare.gov-related meeting in my stead, to accompany me, or help with some aspect of follow-up work. Post October 1, 2013, I asked a former Presidential Innovation Fellow who was an HHS assignee to help assist the effort to turn around the Federally Facilitated Marketplace.

- 16. How many Affordable Care Act Steering Committee meetings were held and how many did you attend? How many of these meetings did the other two co-Chairmen attend?**
- a. Did the Steering Committee stop meeting in early 2013, and if so, why? Did the meetings resume?**
 - b. As co-chairman, what was your role in these meetings?**

Response:

The interagency Steering Committee meetings were organized and led by OMB. My recollection is that they were scheduled to occur on an approximately monthly basis. As I recall, I attended a subset of the meetings, but not all of them. I believe that one or both of the co-chairmen from OMB (or their proxies) attended each of the meetings. (Note: one of the co-chairs, Keith Fontenot, left OMB in early 2013.) With respect to my role on the committee, as discussed earlier, my co-chairs and I provided a neutral venue in which agencies could discuss interagency issues, primarily in support of the data services hub, which ended up going live quite successfully.

My recollection is that in early 2013, the interagency Steering Committee moved to a process in which agencies were to ask co-chair and Federal Chief Information Officer Steve VanRoekel to convene a meeting if any interagency issue arose that required it, whenever required, with monthly meeting times held on calendars in case they should be required for such issues. As I recall, this development was spurred by progress agencies had made on interagency issues, the efficiency with which they were collaborating with each other directly, and the desire to

streamline governance mechanisms (a direction reinforced by the McKinsey “red team” exercise). I can recall a couple of interagency calls that happened subsequent to this development, which I do not believe were spurred by any specific issue, but rather were opportunities for agencies to check in on interagency work in general; my recollection was that agencies indicated that their collaboration was going well.

17. As of the end of August, 2014, you are no longer the U.S. Chief Technology Officer. However, you are still employed by the Administration.

- a. **What is your current formal job title and what are your responsibilities, including to whom do you report?**
- b. **What is your salary and from which office or agency’s budget is it funded?**
- c. **Does your job position require you to file a public financial disclosure report, and if so, which form(s)?**

Response:

My current formal job title is Consultant. My responsibilities are to help attract more and more of the best tech talent in the Nation to serve in government (which is my current primary focus); to identify innovative ways to improve the quality of government digital services and provide advice on their optimal development and operation; and to help ensure that the Administration has an on-the-ground sense of how technology is evolving and can craft policy and initiatives accordingly. Organizationally, I am located in the White House Office; as a practical matter, I work with and for a wide variety of people and agencies across government, including the United States Digital Service, the White House Office of Presidential Personnel, and agencies seeking key tech leadership. I offered and agreed to not receive compensation in this current role, and I am not required to file a public financial disclosure report.

Questions Submitted by House Science, Space, and Technology Committee Ranking Member Eddie Bernice Johnson

1. In his opening, Chairman Broun said, “We have been waiting a very long time to be able to question you, sir. I am sorry that we had to come to the point of issuing you a subpoena to get that to happen, but I am glad that you are here today, sir.” The Chairman continued, “In fact, the Committee has invited you several times before on five different occasions. We wrote directly to you, Mr. Park, as well as to the Director of the Office of Science and Technology Policy. None of those invitations elicited the “yes” response that we got as a result of issuing you a subpoena.” This introduction created the clear impression that you had been avoiding testifying on the Hill. I would like to give you a chance to address this allegation.
 - a. Isn’t it true that you appeared to testify before the House Committee on Oversight and Government Reform on November 13, 2013?
 - b. The White House sent the Subcommittee a letter (Enclosure 5) on September 16, 2014 offering to provide you to testify for a date in November. Despite this voluntary offer to testify you were given a subpoena to appear. In his closing comments, Chairman Broun said, “I am sorry we came to the point where we had to subpoena you to come before this Committee, but thank you for coming, even possibly under duress.” Was a subpoena necessary to get you to testify before the Subcommittee on Oversight on November 19, 2014? Did you appear under “duress?”

Response:

I did testify before the House Committee on Oversight and Government Reform on November 13, 2013. With respect to appearing before the House Science, Space, and Technology Subcommittee on Oversight, I was prepared to testify before the Subcommittee without a subpoena at a mutually convenient date in November 2014, and offered to do so, as indicated by the letter from the White House that the question references.

2. In his opening statement, Chairman Broun questioned the claims of Dr. Holdren that you were not a cybersecurity expert. He described that “as an interesting description of you to say the least.” He continued, “You are the co-founder of athenahealth, which you co-developed into one of the most innovative health IT companies in the industry and become very wealthy in fact doing that. As a government employee, you helped launch the President’s Smarter IT Delivery Agenda, which created the new U.S. Digital Service, and you created the beta version of Healthcare.gov. How do these activities not require cybersecurity expertise?” The Chairman’s rhetorical question deserves an answer.
 - a. Would you please clarify how you could do all the kinds of things the Chairman references and (still) not be a cybersecurity expert?

- b. Please succinctly explain the kinds of specializations that exist in the IT world that may allow someone successful in one area of IT to not necessarily know very much about another area of IT.**
- c. Is it accurate to say that “you created the beta version of Healthcare.gov”, as Chairman Broun asserted? It seems that there is confusion about your work on Healthcare.gov while you were at HHS. Please clarify this matter.**

Response:

As someone who has led technology initiatives both in the private sector and in government, I have learned that the key to success is not to try to do everything yourself, but rather, to assemble the best possible team, composed of remarkable people who have expertise in each necessary area, rally them to a common vision, provide the conditions under which they can do their best work, together, and support them in that work. That is what I did at Athenahealth, where in many areas I relied upon the expertise of others. The world of technology, like many fields of professional endeavor, has developed multiple specialties, as opposed to requiring that everyone be equally adept at everything (which as a practical matter is not possible): specialties including various axes of software development, product management, project management, user experience design, data science, site reliability engineering, hardware and infrastructure engineering, cybersecurity, and more.

With respect to the initial version of HealthCare.gov: as articulated in my written testimony for the November 19, 2014 hearing, in August 2009, I was asked to come serve as the U.S. Department of Health and Human Services’ CTO and “entrepreneur-in-residence.” My role at HHS was to serve as a technology policy and innovation advisor. As a special project, after the passage of the Affordable Care Act in March 2010, I was also asked to lead an early effort to develop a website in 90 days that provided basic information about the Affordable Care Act and health coverage options. This website was the first edition of HealthCare.gov, and was a purely informational site; it did not contain a transactional marketplace in which people applied for health insurance. This early website went live very successfully on July 1, 2010. I should note that this website was subsequently essentially completely replaced in 2013 by the Centers for Medicare and Medicaid Services (CMS) with a new HealthCare.gov that incorporated the Federally Facilitated Health Insurance Marketplace.

3. Chairman Smith stated that, “Mr. Park directed several contractors to review the security of the website.”

a. Did you have the legal or budgetary authority to direct contractors to do any specific work on HealthCare.gov prior to October 1, 2014?

b. Did you ever “direct” any contractors to review security of the website?

Response:

To my knowledge, I did not have the legal or budgetary authority to direct contractors to do any specific work on the new HealthCare.gov and the Federally Facilitated Marketplace prior to October 1, 2013. I do not recall directing any contractors to review the security of the website.

4. You have described your relationship with Henry Chao and CMS in the development of HealthCare.gov as advisory in nature. The records provided to the Committee reflect that very clearly. However, we do not see similar records between you and Tom Shankweiler, the Chief Information Security Officer at HHS who was directing the security development for HealthCare.gov. Prior to October 1, 2013, how would you characterize your relationship with Mr. Shankweiler?

Response:

Prior to October 1, 2013, I can recall being in meetings where Mr. Shankweiler was also present, but had limited direct interaction with him in general.

5. Mr. Park, Chairman Smith led a line of questioning regarding website risks and security and reports. The end result was that Chairman Smith issued a press release with the header, “Park Admits President Knew in Advance about HealthCare.gov problems.” The text of that release does not elaborate in any way on this claim, or provide a particular quote from you, so it is difficult to know what “problems” the Chairman believes the President may have known of from your briefings. However, the claim is clearly rooted in Chairman Smith’s questioning. The Chairman made reference to the Red Team evaluation exercise you participated in and the Mackenzie report, and seemed to suggest that you should have known prior to October 1, 2013 the results of a Government Accountability Office report on cybersecurity of the website that was not available until the Summer of 2014. You did acknowledge briefing senior officials in the White House about the risks identified in the Red Team and Mackenzie reports.

a. Can you succinctly summarize the Red Team and Mackenzie report “risks” and, to the degree you know, briefly describe the actions that were taken to address those risks? Be very clear about which of these risk evaluations, if any, were about cybersecurity.

- b. You mention that you believed there were two briefings for White House senior leadership where the President was in attendance. To the best of your recollection, how many briefings involved the President and when did these occur?**

Response:

The McKinsey “red team” exercise in early 2013 identified both key risks to the Marketplace’s user-facing consumer experience and recommended actions to address those risks, which CMS agreed to adopt, with HHS and White House support. For instance, to address the risk that the Marketplace and Hub would be unavailable due to system failure, the exercise recommended prioritizing and locking down remaining open requirements for version 1.0 of the Marketplace with rapidity, maximizing time for testing, and establishing an operations command center and response capability to deal with post-launch issues. To mitigate the risk that the Federal Marketplace would not be able to absorb large-volume State-based Marketplaces (e.g., NY, CA) at the last minute should those states run into blockers, the exercise recommended communicating with states that they needed to make definitive decisions by a near-term deadline about whether they were going to continue with State-based Marketplaces or go the Federal route. To the best of my recollection and knowledge, none of these key risk evaluations were focused on assessing the cybersecurity defenses of the Marketplace.

With respect to briefings prior to October 1, 2013, with White House senior leadership where the President was in attendance, as referenced in the question, I can recall attending two such briefings – the first in April 2013 and the second in July 2013.

- 6. At times during the hearing, Majority Members used your detailed knowledge about a single, specific matter--for example the effort to get more server capacity on line for October 1--to assert that because you knew that matter so well you must have had detailed knowledge of the project across the board. Please explain again how your role as an advisor for HealthCare.gov put you in a position where you would have detailed knowledge about a specific issue, but still not be in a position to have the kind of detailed information that a day-to-day project manager would have?**

Response:

As I discussed in my testimony, I was not a project manager who was managing and executing the day-in and day-out operational work of building the new HealthCare.gov and the Federally Facilitated Marketplace. This was the responsibility of CMS. I did not have the kind of comprehensive, deep, detailed knowledge of the effort that a hands-on project manager would have, and which I have had about other projects in my private sector work. Prior to October 1, 2013, I assisted CMS with its work in a few different capacities as an advisor, as described in my testimony, while executing my overall duties as White House technology policy and innovation advisor, working on a broad range of policy and innovation matters ranging from open data to fighting human trafficking. With respect to the assistance I provided to CMS, on a particular issue on which my assistance was requested, I would garner particular knowledge on that specific issue at that moment in time; however, I did not have the kind of detailed,

across-the-board, ongoing knowledge of the project that a day-to-day, on-the-ground project manager would have.

- 7. Mr. Johnson made reference to a campaign position advocated by then-candidate (or President-elect) Obama in which it was proposed that a Chief Technology Officer position would be created and, among the examples of their mission said that a CTO would “ensure the safety of our networks” and to ensure the “security of our networks.” Mr. Johnson then made a series of statements that took that proposal from 2008 as a factual statement of your responsibility as CTO. Never were you asked directly if establishing agency-wide cybersecurity standards was included in your portfolio when you came to the CTO job in 2012. Nor did Mr. Johnson mention that the 2002 E-Government Act actually created an office at OMB, the administrator of the Office of Electronic Government (and the two most recent occupants of this position have taken on the title of Chief Information Officer) with responsibility for many aspects of interagency IT policy, including ensuring computer architecture security across the government.**
- a. When you came to the CTO job in March, 2012, were you tasked by the President with ensuring the safety and security of Federal computer networks?**
- b. Based on your experience, was it the CIO at OMB who was charged with interagency cybersecurity responsibilities?**

Response:

When I came to the U.S. CTO job in March 2012, I was not tasked by the President with ensuring the safety and security of Federal computer networks. It is my understanding that it was the CIO at OMB who was charged with interagency cybersecurity responsibilities.

- 8. Mr. Cramer asked you about an email exchange with Ms. Snyder on September 29, 2013. I would like to give you a chance to lay out the context of this email--you mentioned hardware issues during the hearing--and how that was resolved?**

Response:

As I recall, the thrust of the email chain was an effort to bring in additional hardware capacity to reinforce the Marketplace’s ability to support user load. Based on my conversations with CMS management at the time, my understanding of why CMS was moving to add more capacity prior to October 1 was due to the need to expand capacity given load testing results and in anticipation of high demand. CMS asked me to help facilitate getting additional hardware transported to the data center hosting the Marketplace in order to provide additional server capacity; I provided assistance as asked. As discussed earlier, my understanding from CMS was that the additional hardware was successfully transported to the data center and brought online.

9. Compare and contrast your involvement in HealthCare.gov before and after October 1, 2013.

Response:

With respect to the new HealthCare.gov and the Federally Facilitated Marketplace that launched on October 1, 2013: prior to the launch, I assisted CMS with its work in a few different capacities as an advisor, as described in my testimony, while executing my overall duties as White House technology policy and innovation advisor, working on a broad range of policy and innovation matters ranging from open data to the fight against human trafficking. After the launch, as the extent of the operational issues with the site became clear, it became an all-hands on deck moment, and I, along with others, dropped everything else I was doing and increased my involvement in HealthCare.gov dramatically, shifting full-time into the HealthCare.gov turnaround effort, and working as part of the “tech surge” that radically improved the performance of the site. I worked as part of a terrific team, working around the clock, even sleeping on office floors. My particular focus was on helping to reduce the amount of time the site was down, improve the site’s speed, improve its ability to handle high user volume, and improve user-facing functionality. Our team effort drove massive improvement in the site, ultimately enabling millions of Americans to successfully sign up for health insurance through the site.

Enclosure 1

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 you 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]]

Enclosure 2

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

Enclosure 3

Key Points Discussed		
No.	Topic	Highlights
		dependencies from consent.
2	Workgroup Updates	<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

Enclosure 4

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/

Enclosure 5

THE WHITE HOUSE
WASHINGTON

September 16, 2014

The Honorable Paul Broun
Chairman
Subcommittee on Oversight of the
Committee on Science, Space, and Technology
U.S. House of Representatives
Washington, DC 20515

Dear Chairman Broun:

I understand that last Friday the Committee on Science, Space, and Technology's Subcommittee on Oversight (the Subcommittee) noticed a September 17, 2014, business meeting to consider issuing two subpoenas. As described in the notice, the Subcommittee will consider whether to issue a subpoena for Todd Park to appear at a hearing before the Subcommittee, and whether to issue a subpoena for the production of some of Mr. Park's records, during his former tenure in the Office of Science and Technology Policy (OSTP) as United States Chief Technology Officer (CTO), relating to the healthcare.gov website.

I write in advance of the Subcommittee's meeting to ensure you understand that the issuance of these subpoenas is unnecessary. Mr. Park will appear voluntarily for a hearing before the Subcommittee on a mutually convenient date in November to discuss your expressed interest in the healthcare.gov website. OSTP is willing to produce additional documents—including the 102 pages proactively provided with this letter—to further accommodate your "efforts to examine the safety, security and privacy of Americans' personal data through the Obamacare website."¹ The remainder of this letter discusses OSTP's efforts to cooperate with your oversight interests thus far, and OSTP's continued willingness to do so without any need for subpoenas.

I understand that both the full Committee and the Oversight Subcommittee have articulated their interest in the security of healthcare.gov as a desire for information about the measures in place to defend the healthcare.gov website against malicious cyber attacks and to safeguard the personal data of Americans. When Chairman Smith initially wrote to Mr. Park to express interest in healthcare.gov, the letter asked Mr. Park to address "what specific security standards and technical measures are in place to protect Americans' privacy and personal information that passes through the Healthcare.gov website, and what specific steps are in place to mitigate scenarios in which the system is hacked, or personal information is compromised or

¹ Letter from the Hon. Lamar Smith, Paul Broun, M.D., and Larry Bucshon, M.D., to the Hon. John P. Holdren, Director, Office of Science and Technology Policy (December 20, 2013) [hereinafter "December 20 Letter"], at 3.

leaked.”² An email from Committee staff to OSTP at about the same time expressed interest in cybersecurity issues more generally, including a cybersecurity policy report that OSTP Associate Director Patricia Falcone helped prepare.³ In the same vein, your December 20, 2013, letter to OSTP referenced a hearing the Committee held in November of that year to examine the risks that online criminals and identity thieves might pose if they gained access to customers’ personal information.⁴ And more recently in January of this year, the Committee continued its focus on the standards and technical protocols in place to defend against malicious cyber attacks in a second hearing convened on the same topic with “white hat” hackers as witnesses.⁵

From the outset, OSTP has been clear about the limitations both it and Mr. Park face in attempting to respond to the requests for information and testimony concerning these issues involving the development of security standards and the design of scenarios to respond to malicious intrusion attempts. As noted several times in prior correspondence, primary responsibility for those tasks lies elsewhere—with the Centers for Medicare and Medicaid Services (CMS)—and it is CMS that is in the best position to provide complete, current, and accurate information regarding the security protocols in place to protect the website. Nevertheless, the record reflects that OSTP has made substantial efforts to try to accommodate the Committee’s interest in security and to clarify Mr. Park’s role.

OSTP has produced more than one thousand pages of documents; offered on multiple occasions to have Associate Director Falcone testify at a Committee hearing on cybersecurity policy issues; made Mr. Park available for a meeting with you and Chairman Smith in your office, where Mr. Park was willing to address any questions put to him; and offered to have Mr. Park brief all Subcommittee members. Through these substantial efforts at accommodation, OSTP has attempted to help the Committee better understand Mr. Park’s actual duties as the United States CTO and his role with respect to healthcare.gov.

In particular, regarding the documents you have received, your letter of December 20 asked OSTP to produce a very broad set of materials, including all OSTP records concerning the Affordable Care Act and healthcare.gov, scheduling information, records concerning internal White House briefings, and even documents that had not been created but might conceivably be provided to Congress in the future.⁶ Confronted with this broad request and a short deadline in the December 20 letter for responding, OSTP focused its efforts to provide information on the issue that was plainly of particular interest to the Committee, namely, Mr. Park’s participation as one of three co-chairs on the healthcare.gov Interagency Steering Committee. Your December

² Letter from the Hon. Lamar Smith, Chairman, Committee on Science, Space, and Technology, to Todd Park, Assistant to the President and United States CTO (October 31, 2013), at 1.

³ Email from H. Comm. on Science, Space, & Technology Majority Staff to OSTP staff (Oct. 28, 2013, 5:42 p.m.) (“I suspect we would touch on related issues raised and addressed in the ‘Cyberspace Policy Review’ and the Dec 2011 report ‘Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program,’ both of which were referred to in Dr. Holdren’s testimony before the Committee in a full committee oversight hearing on June 20, 2012.”)

⁴ December 20 Letter, at 1 (“The expert witnesses at our hearing outlined the significant risk of identity theft to Americans if hackers gained access to their personal information.”).

⁵ *Hearing Before the H. Comm. on Science, Space, & Tech.*, 113th Cong. (January 16, 2014) [hereinafter, January 16 Hearing].

⁶ December 20 Letter at 3.

20 letter focused on this Steering Committee and its security and privacy subgroup—even going so far as to attach a draft charter for the Steering Committee.⁷

Accordingly, in its January 15, 2014, response, OSTP described the documents it was producing: those concerning the Steering Committee and other interagency meetings that made reference to security, which appeared to be of special interest to the Committee.⁸ OSTP's January 15 letter also explained the interagency coordination function the Steering Committee served, Mr. Park's role in it, and why his participation was not an indication that he had substantial knowledge or expertise concerning the standards or technical protocols for dealing with malicious intrusions that are the focus of the Subcommittee's oversight inquiry. In the eight months following OSTP's production of these documents, the Subcommittee expressed no continued interest in receiving additional documents, nor did it raise any questions concerning the Steering Committee materials provided. Thus, you can understand why the abrupt notice of a business meeting to consider a subpoena for documents came as a surprise.

Despite OSTP's efforts at accommodation, it seems that the push to issue subpoenas this fall may unfortunately reflect a continued misunderstanding of Mr. Park's involvement in the security of the healthcare.gov website. This letter therefore provides additional information, namely, additional OSTP documents beyond those already provided concerning the Interagency Steering Committee, concerning Mr. Park's limited involvement in the security aspects of the website, which are primarily handled by CMS. The enclosed documents can be grouped into three categories.

First, in an extension of his role with the Steering Committee, Mr. Park, and his other co-Chairs were occasionally asked to assist in instances when White House personnel made requests to officials at HHS and CMS. One instance when such assistance was sought involved a request for a meeting on user credentialing and identity-proofing from National Security Staff and Office of Management and Budget officials. The documents themselves make clear that although the particular request for assistance was made from CMS officials to Mr. Park, it was another co-Chair who provided assistance in addressing that request.⁹

Second, Mr. Park was asked on a small number of occasions to assist in obtaining information from CMS and HHS personnel responsible for security of the website. In that role, Mr. Park asked HHS and CMS officials to develop background points describing the cybersecurity protections and helped coordinate follow-up conversations between the HHS and CMS officials and cybersecurity experts both inside and outside the government. Again, the emails themselves show that Mr. Park was not directly familiar with the development of

⁷ See also *January 16 Hearing* (statement of Rep. Paul Broun, M.D.) ("It's probably [sic] the oversight committee of—subcommittee of this committee's attention that there is—or at least was [an] Affordable Care Act information technology exchanges steering committee [chaired] by senior White House officials established back in May 2012, almost a year and a half before the roll out of Healthcare.gov.").

⁸ Letter from the Donna Pignatelli, Director, OSTP Legislative Affairs, to the Hon. Lamar Smith, Chairman, Committee on Science, Space, and Technology (January 15, 2014) [hereinafter January 15 Letter], at 3. At Chairman Smith's request, OSTP also produced all documents that it had at that point provided to the Committee on Oversight and Government Reform.

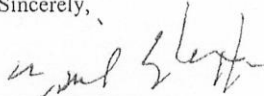
⁹ Email from Steven VanRoekel to J. Michael Daniel, et al. (Apr. 12, 2013, 3:25 p.m.), enclosed.

cybersecurity defenses in place, but instead served as an intermediary and relied on the HHS and CMS officials to provide the substance of the information he then passed on to others.¹⁰

Third, shortly before the first open enrollment period, Mr. Park also served as a liaison with cybersecurity officials at HHS and CMS in connection with efforts to explain publicly the cybersecurity protections for the health insurance marketplaces. This “spokesman” function is one Mr. Park performed from time to time as CTO with respect to technology issues generally. Importantly, the enclosed emails again confirm that Mr. Park was not speaking from direct personal knowledge or experience on cybersecurity—before participating in a press call, he solicited the relevant information from CMS cybersecurity personnel and sought to have them participate in the call given his relative lack of familiarity with cybersecurity issues.¹¹

The information provided in and with this letter is consistent with what OSTP has previously explained: that CMS is best positioned to address the Subcommittee’s questions regarding the security of the website and that Mr. Park has not been substantially involved in developing or managing the “specific security standards and technical measures . . . in place to protect Americans’ privacy and personal information that passes through the Healthcare.gov website” More importantly, if the Subcommittee desires additional information, there is no need to resort to subpoenas. Mr. Park will be pleased to testify at a Subcommittee hearing in November. OSTP is also actively searching for additional records that may further illuminate Mr. Park’s relatively minor role on cybersecurity issues and is willing to voluntarily produce additional documents to aid the Subcommittee’s inquiry. Please simply have your staff communicate the Subcommittee’s priorities in that regard to OSTP.

Sincerely,



W. Neil Eggleston
Counsel to the President

¹⁰ Email from Todd Park to Tony Trenkle, et al. (Sept. 2, 2013, 1:14 p.m.), enclosed (“Hi Tony, many apologies for interrupting your Labor Day, but can you help Chris with his follow-up question below (reference to ‘current federal standards and how they exceed private sector as well as track record of protection from attacks’).”).

¹¹ Email from Todd Park to Tony Trenkle, et al. (Sept. 17, 2013, 9:54 p.m.), enclosed (“I’ve let Jessica know that you guys are the font of detailed knowledge on CMS/HHS cyber and that I can talk to it at a general level only -- she thinks that will be OK on the call tomorrow, with detailed questions to be referred to agencies.”).