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

HEARING CHARTER

The Role of the White House Chief Technology Officer in the HealthCare.gov Website Debacle

Wednesday, November 19, 2014
10:00 a.m. – 12:00 p.m.
2318 Rayburn House Office Building

Purpose

On Wednesday, November 19, 2014, the Subcommittee on Oversight will hold a hearing titled, *The Role of the White House Chief Technology Officer in the HealthCare.gov Website Debacle*.

On September 17, 2014, the Subcommittee on Oversight approved a resolution to authorize the issuance of a subpoena *ad testificandum* to Mr. Todd Park, former Chief Technology Officer (CTO) of the United States, Office of Science and Technology Policy (OSTP). The subpoena compels Mr. Park's appearance before the Subcommittee to explain his role in the development and rollout of the HealthCare.gov website that Health and Human Services (HHS) Secretary Kathleen Sebelius called a "debacle"[1] with a recently estimated cost of over $2 billion.[2] Despite Mr. Park denying knowledge of security and testing concerns with HealthCare.gov prior to the rollout of the website, the Committee has reviewed many emails where Mr. Park demonstrates an in-depth knowledge of these issues prior to October 1, 2013. This hearing will cover what Mr. Park knew and what he reported to other senior White House officials.

In late August, the White House announced that Mr. Park would step down as CTO to take a new role in the Administration as technical advisor to the White House, working from Silicon Valley.

Witness

- **Mr. Todd Park**, former Chief Technology Officer of the United States, Office of Science and Technology Policy

[1] Bill Chappell, "Sebelius Calls For Review of HHS Practices That Led To Debacle," NPR, December 11, 2013, available at: http://www.npr.org/blogs/thetwo-way/2013/12/11/250207327/sebelius-calls-for-review-of-hhs-practices-that-led-to-debacle.
[2] Alex Wayne, "Obamacare Website Costs Exceed $2 Billion, Study Finds," Bloomberg, September 24, 2014, available at: http://www.bloomberg.com/news/2014-09-24/obamacare-website-costs-exceed-2-billion-study-finds.html.

Background

As U.S. CTO, Mr. Park declined five invitations to testify before the Committee about his knowledge and involvement with the development of HealthCare.gov, including its cybersecurity standards and protocols. Over the course of several letters, OSTP has claimed:

- It "has not been substantially involved in the privacy and security standards that are in place for healthcare.gov."[3]

- Neither "Mr. Park nor any other OSTP staff member is in a position to testify on the data security standards of the website. Indeed, when asked about the security features of the HealthCare.gov website during a hearing…before another committee, Mr. Park explained that he has not been working on these issues."[4]

- Mr. Park and "OSTP personnel have not been substantially involved in developing or implementing the Federally Facilitated Marketplace's (FFM) security measures.…Mr. Park is not a cybersecurity expert; he did not develop or approve the security measures in place to protect the website, and he does not manage those responsible for keeping the site safe."[5]

Further, while testifying under oath when subpoenaed by the Oversight and Government Reform Committee last November, Mr. Park said that he did not "actually have a really detailed knowledge base" of the website before it was launched and was "not deeply familiar with the development and testing regimen that happened prior to October 1."[6]

However, documents received by the Science Committee over the summer and this past month from the Committee's subpoena of Mr. Park's records raise serious questions of Mr. Park's denial that he was not knowledgeable or familiar with the development, testing, and security concerns relative to the HealthCare.gov website.

HealthCare.gov

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 as well as 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

---

[3] November 8, 2013, Letter from OSTP to SST Committee.
[4] November 14, 2013 Letter from OSTP to SST Committee.
[5] July 3, 2014, Letter from OSTP to SST Committee.
[6] "Obamacare Implementation – The Rollout of HealthCare.gov," House Oversight and Government Reform Committee, November 13, 2013, available at: http://oversight.house.gov/hearing/obamacare-implementation-rollout-healthcare-gov.

personal contact information, birth dates and social security numbers for all family members, in addition to household salary, and other personal data.

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,[7] and cybersecurity experts at a November 2013 hearing before the Science Committee expressed concern about flaws in the website that put the personal data of Americans using the website at risk of identity theft from cybercriminals/hackers.[8]

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

On October 31, 2013, the Committee sent the first letter to Mr. Todd Park, then-U.S. 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. The Committee's specific interest in questioning Mr. Park was based on several factors:

- 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 worked at OSTP and was considered part of OSTP leadership. While there he focused on "how technology policy and innovation can advance the future of our nation."[11] According to his biography, previously available on OSTP's website, 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 two years ago, Dr. John Holdren, OSTP Director, explained that:

---

[7] 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.

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

[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, previously available at: http://www.whitehouse.gov/administration/eop/ostp/about/leadershipstaff/park.

[12] Ibid.

[13] Ibid.

> "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]

The Science Committee's interest in hearing from Mr. Park intensified with the acquisition of documents from the Oversight and Government Reform Committee that identified Mr. Park as a White House co-chair of the Affordable Care Act Information Technology Exchanges Steering Committee.[15] According to these documents, 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 its 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.

Previous Hearings

When the site was launched on October 1, 2013, it was plagued with operational problems. In light of the myriad 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.[16] 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.

The Committee revisited these issues in a subsequent hearing on January 16, 2014,[17] 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. At the conclusion of the hearing, Chairman

---

[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.

[15] SST Majority Staff Report, "Did the White House Knowingly Put Americans' Sensitive Information at Risk? Committee Seeks to Clarify Contradictions Surrounding Senior White House Official's Role in Developing HealthCare.gov," October 2014, available at: http://science.edgeboss.net/sst2014/documents/October%202014%20Todd%20Park%20Majority%20Staff%20Report.pdf.

[16] 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.

[17] 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.

Smith called on the President to formally certify the safety requirements, security standards and privacy conditions of HealthCare.gov.

Questions Remain

One year later, concerns about the HealthCare.gov website's security still remain with the second Open Enrollment period for HealthCare.gov. Despite the improved functionality since the flawed October 1st launch, it is unclear how much work has been done to address the privacy and security aspects of that functionality, which were concerns raised in the Committee's prior 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."[18]

- News stories in September also reported that a "hacker broke into part of the HealthCare.gov insurance enrollment website in July and uploaded malicious software."[19]

- A recent U.S. Government Accountability Office review of the website made the following observation: "Healthcare.gov had weaknesses when it was first deployed, including incomplete security plans and privacy documentation, incomplete security tests, and the lack of an alternate processing site to avoid major service disruptions."[20] This report also finds: "[W]eaknesses remain both in the processes used for managing information security and privacy, as well as the technical implementation of IT security controls."[21]

- And in a recent news conference, the President reportedly said, "We're really making sure the website works super well before the next open enrollment period. We're double-and triple-checking it."[22] However, the same news article reports that while HealthCare.gov performed better than last year, consumers in Virginia for example, "were having a hard time logging into their accounts retrieving old passwords and proving they were who they said they were – a process known as identity proofing, which also vexed many people last fall."[23]

---

[18] 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.
[19] 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.
[20] "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.
[21] Ibid.
[22] Robert Pear and Abby Goodnough, "Some New Frustrations as Health Exchange Opens," New York Times, November 15, 2014, available at: http://www.nytimes.com/2014/11/16/us/health-insurance-marketplace-opens.html?rref=us&module=ArrowsNav&contentCollection=U.S.&action=keypress&region=FixedRight&pgtype=article.
[23] Ibid.