ONE HUNDRED THIRTEENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515–6143

MAJORITY (202) 225–5074
FACSIMILE (202) 225–3974
MINORITY (202) 225–5051

http://oversight.house.gov

January 8, 2014

The Honorable Kathleen Sebelius
Secretary
U.S. Department of Health & Human Services
200 Independence Avenue, SW
Washington, D.C. 20201

Dear Madam Secretary:

The Committee is conducting oversight of the Obama Administration's implementation of the Affordable Care Act, commonly referred to as "ObamaCare." One particularly troubling aspect of this issue is that senior Department of Health and Human Services officials knew, or should have known, that the rollout of HealthCare.gov was fraught with risks but launched the website anyway.

You attempted to address these and other concerns about the implementation of ObamaCare in testimony before the Congress. Your testimony before the House Committee on Energy and Commerce was that no senior HHS official ever advised you to delay the rollout of the federal health insurance enrollment system. You also testified to the Senate Finance Committee that, in advance of the rollout, no one suggested that security risks outweighed the importance of moving forward with bringing the enrollment system online.

Documents and testimony obtained by the Committee, including information provided by Teresa Fryer, the Chief Information Security Officer at the Centers for Medicare and Medicaid Services (CMS), and the MITRE Corporation, a contractor hired by HHS to conduct security assessments of HealthCare.gov, show that your testimony was false and misleading. Prior to further investigative action by the Committee, we thought it prudent to write to you and invite you to reflect on your testimony. Should it be necessary to clarify or amend your testimony, then we request you do so as quickly as possible.

Hearing Testimony

First, on October 30, 2013, you had the following exchanges with Congressman G.K. Butterfield (D-NC) and Congressman Gus Bilirakis (R-FL) before the House Energy and Commerce Committee:

Mr. Butterfield: My understanding is that an independent security expert, the MITRE Corporation, is performing security testing on the code that powers the website on an ongoing basis, is that correct?

You: That is correct, and MITRE did an assessment of the system, gave us a preliminary report, they are in the process of posting their final report. That did not raise flags about going ahead, and the mitigation strategy was put in place to make sure that we had a temporary authority to operate in place while the mitigation was going on, and then a permanent authority to operate will be signed.[1]

* * *

Mr. Bilirakis: Did any senior department official predict serious problems? And did any senior department officials advise delaying the rollout of the exchanges or parts of the exchanges on October 1st? Could you . . .

You: I can tell you that no senior official reporting to me ever advised me that we should delay.

Second, on November 6, 2013, you had the following exchange with Senator Hatch (R-UT) before the Senate Finance Committee:

Sen. Hatch: Did anybody brief you on the security risks?

You: We discuss security as part of the overall operations on a regular basis with the operations team, but no one, I would say, suggested that the risks outweighed the – the importance of moving forward, including our independent evaluator, MITRE, who made recommendations to CMS, as is required.[2]

Documents and Witnesses Contradict Your Hearing Testimony

Based on the documents and information gathered during the Committee's investigation, it is apparent that your Congressional testimony on these two occasions was false and misleading.

---

[1] *PPACA Implementation Failures: Answers from HHS: Hearing before the H. Comm. On Energy and Commerce*, 113th Congress (October 30, 2013) (statement of Sec. Kathleen Sebelius)
[2] *Health Insurance Exchanges: An Update from the Administration: Hearing before the Sen. Comm. on Finance*, 113th Congress (November 6, 2013) (statement of Sec. Kathleen Sebelius)

First, your affirmative response that MITRE was conducting security testing of the website on an ongoing basis was false.

MITRE and Blue Canopy, the contractors utilized by CMS to conduct security testing of HealthCare.gov and its related components, did not conduct ongoing security testing of the system. According to Ms. Fryer's testimony, MITRE's final round of security testing on the federal exchange prior to the October 1, 2013, launch ended on September 20, 2013.[3] MITRE delivered a preliminary report to CMS on September 23, 2013, that was based on that round of security testing.[4] Blue Canopy delivered its draft security assessment test prior to the October 1, 2013, launch, on September 30, 2013.[5] MITRE and Blue Canopy did not begin work on another security control assessment of the federal exchange until December 10, 2013 – ten weeks after the system launched on October 1, 2013.[6]

Second, your statement that MITRE's preliminary report "did not raise flags about going ahead" is false.[7]

Ms. Fryer, possibly the only senior HHS or CMS official who reviewed MITRE's preliminary report, was very concerned about the problems raised by MITRE during its security testing of the system.[8] According to MITRE's report, "MITRE was unable to adequately test the Confidentiality and Integrity of the [Exchange] system in full."[9] MITRE's report identified many specific problems that led to their inability to adequately test the Exchange prior to the October 1, 2013 launch:

- "[K]nown functional limitations and omissions due to the software still being developed."[10]
- Some environments "not vetted or tested by CMS or the development contractor prior to the onsite assessment to ensure the HIX workflows were functional."[11]
- "Test data manually entered by MITRE, in most instances, was unable to be validated as needed by the workflow to allow testing to proceed to the next step in the HIX Workflows."[12]

---

[3] Transcribed interview of Teresa Fryer, Ctr. for Medicare and Medicaid Services (CMS), in Wash. D.C. at 106 (Dec. 17, 2013). [hereinafter "Fryer"]
[4] MITRE HIX Security Control Assessment Draft Report (September 23, 2013) [00791-00897]
[5] Blue Canopy HIX-A Security Control Assessment Draft Report (September 30, 2013) [BCI020955-BCI020989]
[6] Fryer at 220.
[7] *PPACA Implementation Failures: Answers from HHS: Hearing before the H. Comm. on Energy and Commerce*, 113th Congress (October 30, 2013) (statement of Sec. Kathleen Sebelius)
[8] Fryer at 231.
[9] MITRE HIX Security Control Assessment Draft Report (September, 23, 2013) [00791-00897]
[10] *Id.*
[11] *Id.*
[12] *Id.*

- "Test environment availability was not consistent. Several times during the [Security Control Assessment] the testing environments "went down" due to DSH, EIDM, or HIOS systems being taken off line or rebooted. These events would occur without warning and only after the systems were taken off line was MITRE informed. This caused many outages and black out windows for [Security Control Assessment] testing because the system was functionally unusable."[13]

- "Environments were not dedicated to [Security Control Assessment] testing."[14]

- "CMS instructed MITRE that SCA efforts to interrupt the availability of the system, such as attempting Denial of Service exploits, were not to be performed. Due to this limitation MITRE was unable to determine the ability of HIX to withstand such attacks by a malicious user."[15]

Although the independent security testing raised several significant security vulnerabilities, Ms. Fryer's primary concern was the vulnerabilities that were unknown from the failure to conduct a complete security test prior to October 1, 2013.[16] In preparation for a September 23, 2013, security briefing, Ms. Fryer prepared a PowerPoint slide that listed two high risks with opening the Exchange on October 1, 2013. The two "unknown" risks identified by Ms. Fryer, which confronted individuals who entered their information into HealthCare.gov beginning on October 1, 2013 were:

- Unknown risk of applications to withstand attacks aimed at system availability.

- Unknown risks associated with those controls and those functionalities that were not tested.[17]

During the transcribed interview on December 17, 2013, Ms. Fryer was asked about the two high findings of risk that she identified:

> Q Were you more concerned with the unknown risks because of the insufficient testing than the specific risks that were identified by MITRE?
>
> A I was concerned about, yes, the unknowns, the uncertainties from the issues that were raised, again, about [conducting security testing in] the different environment [with] different versions of the code that led to a level of uncertainty rather than the actual risks that were identified.

---

[13] *Id.*
[14] *Id.*
[15] *Id.*
[16] Fryer at 34.
[17] Marketplace Security Briefing, September 23, 2013 [HHSHOGR12.16.13000000000000004]

* * *

Q -- the first risk is, "Unknown risk of applications to withstand attacks aimed at system availability," and there's a dash that says "high risk."

A Yes.

Q Who identified this as a high risk?

A I did.

Q And the second one, "Unknown risks associated with those controls and those functionalities that were not tested." Did you also identify that as a high risk?

A Yes.

Q So, in your opinion, the system on October 1st had a high risk when it went live?

A From a security perspective, for a security risk only, in my opinion, yes, it was a high risk because of the level of uncertainty discovered during the testing.[18]

Ms. Fryer also testified that there were ways to reduce the security risks involved with the launch of the website:

Q So there were ways to reduce the number of unknown risks?

A Yes.

Q And one way would be to test in a single environment. So testing in a single environment would have reduced the number of unknown risks that were present on October 1st?

A Yes.

Q And dedicated security testing also would have reduced the number of risks that were present on October 1st?

A It would have reduced the level of uncertainty, yes.[19]

[18] Fryer at 156.

However, dedicated security testing in a single environment did not occur prior to October 1, 2013. Presumably, these steps to reduce the risk would have been achievable if the Administration was open to delaying the launch of ObamaCare past October 1, 2013. But, it appears that the Administration was so intent on opening HealthCare.gov that the decision was made to proceed with an insecure and largely untested website.

Third, your statement that, "no one … suggested that the risks outweighed the – importance of moving forward" is false.[20]

Ms. Fryer, the senior CMS official involved with security testing, testified that she recommended a denial of the authority to operate (ATO) for the Exchange to open on October 1, 2013, due to concerns about the high risks associated with a lack of testing. On September 20, 2013, during a conference call with other senior CMS and HHS information and security officials, Ms. Fryer recommended a denial of the ATO for HealthCare.gov to open on October 1, 2013:

> Q. So this recommendation in slide 5, "Follow the mitigation plan and issue an interim ATO," do you know whose recommendation that is?
>
> A. No, I don't.
>
> Q. Is that your recommendation?
>
> A. No, it's not.
>
> Q. Would it have been your recommendation?
>
> A. No.
>
> Q. What would your recommendation have been?
>
> A. My recommendation was a denial of an ATO.
>
> Q. Who did you make that recommendation to?
>
> A. To my management. To the authorizing official.
>
> Q. Which is who?

---

[19] Fryer at 158.

[20] *Health Insurance Exchanges: An Update from the Administration: Hearing before the Sen. Comm. on Finance*, 113th Congress (November 6, 2013) (statement of Sec. Kathleen Sebelius)

A. Tony Trenkle [at the time CMS's Chief Information Officer].

Q. And did you do that in person?

A. Yes, and it was during the security testing when the issues were coming up about the availability of the system, about the testing in different environments. I had discussions with him on this and told him that my evaluation of this was a high risk.

Q. And did those discussions occur -- was it just the two of you when you gave him that recommendation?

A. In the beginning, yes, and then we also briefed HHS.

Q. Who at HHS?

A. Frank Baitman [HHS's Chief Information Officer] and Kevin Charest [HHS's Chief Information Security Officer].

Q. Do you recall when you made that recommendation to Mr. Trenkle?

A. No, I can't recall the date.

Q. Was it prior to September 23rd?

A. Yes.

* * *

Q.: So you had an in-person meeting with you, Mr. Trenkle, and you spoke with Frank Baitman and Kevin Charest. Is that right?

A. On a telecon[ference], yes.

Q. Telecon[ference]. Do you recall when that was?

A. September 20th.

* * *

Q. Okay. And so you recommended denying the ATO during that call?

A. Yes.

* * *

Q. Did [Mr. Trenkle] share your concerns?

A. Yes, he did.[21]

On September 23, 2013, three days after Ms. Fryer discussed her denial of an ATO for HealthCare.gov with Mr. Baitman, Mr. Charest, Mr. Trenkle, and Mr. Henry Chao, the day-to-day operational lead at CMS for HealthCare.gov, a meeting was convened at CMS to discuss the security risks.[22] Shockingly, according to Ms. Fryer, neither she, nor anyone from her security testing oversight team, was present at the meeting, which focused on security concerns with the Exchange and HealthCare.gov.[23] During the meeting and its aftermath, a strategy emerged for how to issue the authority to operate for HealthCare.gov.

On September 24, 2013, after learning of the decision that an ATO for the federal Exchange would be sent to CMS Administrator Tavenner, Ms. Fryer drafted a memorandum that listed her concerns with launching HealthCare.gov on October 1, 2013.[24] According to the memorandum drafted by Ms. Fryer, the Exchange "does not reasonably meet the CMS security requirements. … **There is also no confidence that Personal Identifiable Information (PII) will be protected.**"[25] [Emphasis Added] In the draft memorandum, Fryer also explained that "[o]f the seventeen modules documented for [the Exchange], eight modules were not fully security assessed."[26]

Standard security practice is for the Chief Information Officer to sign ATO documents.[27] Therefore, Tony Trenkle should have been the authorizing authority in this instance, but he refused to sign the ATO for HealthCare.gov to open on October 1, 2013.[28] In response to questioning, Ms. Fryer testified that the ATO was left for Ms. Tavenner to sign after Mr. Trenkle refused:

Q. Who -- who signed the ATO to open up the marketplace?

A. Marilyn Tavenner signed the risk decision memo, yes.

---

[21] Fryer at 163.
[22] Fryer at 171.
[23] *Fryer*, transcribed interview of Henry Chao, CMS, in Wash. D.C. (Nov. 1, 2013), transcribed interview of Tony Trenkle, CMS, in Wash. D.C. (Dec. 4, 2013)
[24] Risk Decision for the Federally Facilitated Marketplace (September, 24, 2013) [HHSHOGR12.20.1300000000000010]
[25] *Id.*
[26] *Id.*
[27] Fryer at 169.
[28] *Id.* at 84.

Q. Okay. So, your boss, who you briefed, who you said this was high risk, did not sign the document?

A. Yes.

Q. And in ordinary course, he would have been the person expected to sign the document; is that correct?

A. Expected to sign an authority to operate, yes, he is the authorizing official.[29]

According to testimony from all the witnesses interviewed by the Committee to date, it is unprecedented for a CMS Administrator to sign an ATO, and Ms. Tavenner's signature on the September 27, 2013, ATO to open HealthCare.gov was the first time anyone could recall a CMS Administrator ever signing an ATO.[30]

Ms. Fryer testified that despite her recommendation of a denial of the ATO, she was asked to put her name on the ATO document.[31] Ms. Fryer testified that she was not comfortable doing so and refused:

Q. What was the wording that you refused to sign?

A. That it said all parties recommend a six-month ATO.

Q. And did you communicate your refusal to sign that document via email?

A. Yes.

Q. To who?

A. George Linares [CMS's Chief Technology Officer].

Q. Did Mr. Linares respond to your email?

A. Yes. He wanted to know what my concerns were.

Q. And did you express your concerns?

A. Yes.

---

[29] *Id.* at 84.
[30] Fryer, transcribed interview of Henry Chao, CMS, in Wash. D.C. (Nov. 1, 2013), transcribed interview of Tony Trenkle, CMS, in Wash. D.C. (Dec. 4, 2013)
[31] Fryer at 190-191.

Q. What did you express to him?

A. I said that I could acknowledge the level of risk but not concur with the recommendation for a six-month ATO.[32]

After refusing to agree with the recommendation for a six-month ATO for the Exchange, Ms. Fryer testified that she was willing to sign a different document with the following language:

> We acknowledge the level or risk the Agency is accepting in the Federally Facilitated Marketplace (FFM). **The mitigation plan does not reduce the risk to the FFM system itself going into operation on October 1, 2013.** However, the added protections do reduce the risk to the overall marketplace operations and will ensure that the FFM system is completely tested within the next six months.[33] [emphasis added]

In addition to Ms. Fryer, Mr. Trenkle and Michelle Snyder, CMS's Chief Operating Officer, signed the alternative document.[34] Ms. Fryer made clear in her interview that the mitigation plan did not address the unknown risks to individuals that existed because of the failure to conduct adequate security testing.[35] Ms. Fryer responded affirmatively when asked if "it's difficult to have a mitigation plan when you don't do the testing and aren't sure what the risks are."[36] She stated that, "usually a mitigation plan or remediation plan is put into place after findings are discovered."[37] While Fryer testified that CMS did come up with "extra protections" for the site as a whole, she noted, "we couldn't mitigate or remediate those unknown risks."[38]

Fourth, your statement that MITRE made recommendations to CMS about moving forward with the launch on October 1, 2013 is false.[39]

According to MITRE, "MITRE was not informed, nor asked, by CMS about a "go-ahead" for HealthCare.gov."[40]

Correcting the Record

Although the four examples of misinformation and falsehoods from your Congressional testimony late last year are extremely troubling, your failure during numerous Congressional

---

[32] *Id.*
[33] Risk Acknowledgement Signature Page (September 27, 2013) [CGIHR00002835]
[34] *Id.*
[35] Fryer at 174.
[36] *Id.*
[37] *Id.*
[38] *Id.*
[39] *PPACA Implementation Failures: Answers from HHS: Hearing before the H. Comm. On Energy and Commerce*, 113th Congress (October 30, 2013) (statement of Mrs. Kathleen Sebelius)
[40] Email from MITRE counsel to staff, H. Comm. on Oversight and Gov't Reform (November 12, 2013)

hearings to explicitly mention the serious problems with security testing in the month prior to launch creates the appearance that you carefully chose language that would mislead Members of Congress and the American public.

For example, you failed to mention how the chaotic development process throughout August and September limited the effectiveness of the security testing. You also failed to mention that several functionalities went live on October 1, 2013, without being subject to any security control assessment from either MITRE or Blue Canopy.

Your testimony on October 30, 2013, before the Energy and Commerce Committee created the impression that senior HHS officials—including you—were never advised to delay the rollout of HealthCare.gov. This is not true. We now know that a senior official at CMS advised delay because of security concerns and that she conveyed her recommendation to two senior HHS officials.

Finally, on December 11, 2013, one day after MITRE and Blue Canopy began the first Security Control Assessment on the Exchange after October 1, 2013, you testified before the Energy and Commerce Committee on ObamaCare failures.[41] It is noteworthy that the independent security testing conducted that week and the next week identified at least two high findings of risks associated with HealthCare.gov.[42]

Q. Just to be clear, these are two new high findings that were not previously identified by MITRE or anybody else?

A. One high finding was identified in an incident that was reported in November.

* * *

Q. Do you know if these -- were these high findings, do you know how long they were in existence in the system?

A. No, I don't know.

Q. So it's possible they have been in the system since October 1st?

A. Again, I can't speculate. [43]

Providing false or misleading testimony to Congress is a serious matter. Witnesses who purposely give false or misleading testimony during a congressional hearing may be subject to

---

[41] *PPACA Implementation Failures: What's Next: Hearing before the H. Comm. on Energy and Commerce*, 113th Congress (December 11, 2013) (statement of Mrs. Kathleen Sebelius)
[42] *Id.* at 225.
[43] *Id.* at 227.

criminal liability under Section 1001 of Title of 18 of the U.S. Code, which prohibits "knowingly and willfully" making materially false statements to Congress.[44] With that in mind, I write to request that you correct the record and to implore you to be truthful with the American public about matters related to ObamaCare going forward. In addition, in order to determine the full extent of other officials' roles in developing your recent Congressional testimony, I request you provide copies of all documents and communications, including meeting notes, prepared for your three appearances before Congress after October 1, 2013.

The Committee on Oversight and Government Reform is the principal oversight committee of the House of Representatives and has broad authority to investigate "any matter" at "any time" under House Rule X.

If you have any questions about this request, please contact Brian Blase of the Committee at (202) 225-5074. Thank you for your attention to this important matter.

Sincerely,

Darrell Issa
Chairman

Enclosure

cc: The Honorable Elijah E. Cummings, Ranking Minority Member

[44] 18 U.S.C. §1001 states, in pertinent part: [W]hoever, in any matter within the jurisdiction of the executive, legislative, or judicial branch of the Government of the United States, knowingly and willfully—(1) falsifies, conceals, or covers up by any trick, scheme, or device a material fact; (2) makes any materially false, fictitious, or fraudulent statement or representation; or (3) makes or uses any false writing or document knowing the same to contain any materially false, fictitious, or fraudulent statement or entry; shall be fined under this title, [or] imprisoned not more than 5 years . . . .