U.S. House of Representatives

Committee on Oversight and Government Reform

Darrell Issa (CA-49), Chairman

Behind the Curtain of the HealthCare.gov Rollout

MAJORITY STAFF REPORT
U.S. HOUSE OF REPRESENTATIVES
113TH CONGRESS
SEPTEMBER 17, 2014

Table of Contents

EXECUTIVE SUMMARY

The Obama Administration entrusted the Centers for Medicare and Medicaid Services (CMS) with the lead role in the implementation of the Patient Protection and Affordable Care Act, or ObamaCare. Within CMS, the Center for Consumer Information and Insurance Oversight (CCIIO) was responsible for developing and operating the federally-facilitated exchange, or federally-facilitated market place (FFM), in the 36 states that declined to set up their own state exchange.

In what would prove to be a very prescient observation, on May 11, 2010, Jonathan Gruber, considered by many as an architect of ObamaCare, questioned whether the Administration could get the job done: "I do not believe the relevant members of the Administration understand the President's vision or have the capability to carry it out."[1] In particular, Mr. Gruber singled out CMS, writing that "[t]he agency is demoralized, the best people have left, [and the] IT services are antiquated ...."[2] Part of Mr. Gruber's concerns can be illustrated by the launch of the law's first open enrollment season. After more than three years of development at CMS, Healthcare.gov crashed almost immediately. As a result, users experienced long wait times, errors, bugs, and other problems.

For the past four years, the Oversight and Government Reform Committee has conducted vigorous oversight of the implementation of ObamaCare, including the disastrous launch of Healthcare.gov. The problems regarding CMS's failure to launch a functioning website are consistent with broader issues in transparency and accountability within the Administration. Officials at CMS and HHS refused to admit to the public that the website was not on track to launch without significant functionality problems and substantial security risks. There is also evidence that the Administration, to this day, is continuing its efforts to shield ongoing problems with the website from public view.

Despite its position within the Department of Health and Human Services (HHS), the CMS development team resisted greater involvement from senior HHS officials, opting to bypass HHS and instead work through Senior White House official Todd Park. The broken lines of communication between CMS and HHS continued throughout the project's development. Eventually, CMS shared so little information that Bryan Sivak, HHS Chief Technology Officer, sought informal reports from former HHS employees tasked to CMS to help with Healthcare.gov, often communicating over non-official, private email. The hostility between CMS and HHS ultimately proved detrimental to the project. For example, after Mr. Sivak received evidence from an informant that Healthcare.gov was not ready to launch on October 1, 2013, Mr. Sivak and other senior HHS IT officials suggested a phased launch, or Beta launch, instead of launching the website nationwide. This suggestion was ignored by senior HHS and CMS leadership.

In addition to conflicts between CMS and HHS, documents obtained by the Committee show hostile factions within CMS itself, particularly over website security. Teresa Fryer, CMS

[1] Memorandum from David Cutler, to Larry Summers (May 11, 2010), *available at* http://www.washingtonpost.com/blogs/wonkblog/files/2013/11/Cutler-implementation-memo-1.pdf.
[2] *Id.*

Chief Information Security Officer, testified that other CMS officials obscured the true nature of the security problems in the days leading up to the launch: "[O]ur job as security experts is to portray the posture or the events that are happening and to brief senior leadership management on the security issues that are being raised during testing. And I felt that they were not being properly briefed or properly portrayed, the issues that were happening that week during security testing."[3] Ms. Fryer's team was challenged by Thomas Schankweiler, an Information Security Officer at CMS, who led security efforts for the CMS team responsible for the development of the FFM. When the MITRE Corporation's independent assessment of the website showed significant problems with the website's security, Mr. Schankweiler criticized the accuracy of the report and sought to change it.

The federal exchange launched on October 1, 2013, despite concerns raised by Ms. Fryer. CMS went through an unprecedented process in order to authorize the exchange: for the first time, Administrator Marilyn Tavenner, instead of the Chief Information Officer, signed the document authorizing the system to go live and launched the website. Rather than being transparent about this process, CMS sought to hide this from state partners and other oversight entities. These examples illustrate a larger pattern of deception surrounding the Administration's implementation of ObamaCare.

Although many of these problems originated with CMS, it is HHS and the Administration who ultimately bear responsibility for the failures with the agency's poor management and oversight. The frustration with the Administration's lack of accountability can best be summed up in a November 2013 email sent by an HHS employee to Mr. Sivak:

> Here is what I don't understand. Is there some misunderstood 'understanding' going on here? I mean it is a complete embarrassment for the President to get up and say 'he never knew' that there was [sic] problems prior to Oct. 1. Either that is a lie (I don't particularly believe he is a blatant liar) or his staff is not communicating. I mean you knew it, but your leadership only wanted to hear beautiful music and talk about rainbows and unicorns. [United States Chief Technology Officer] Todd [Park] had to have known it, but somehow he had the utmost faith in [CMS Deputy CIO] Henry [Chao] and team. I'm just totally missing how it got to this point. And I don't mean the technical delivery…I mean the out and out incompetence. Unless it is some sort of conspiracy…Maybe the House of Cards is real! But clearly, these people are not smart enough to pull it off. So, yeah, I'm a little confounded. How did one week Henry Chao tell us there was no way Account Transfer would be ready, then a meeting at the White House and a week later, oh, yeah, everything is back on track, we'll meet the dates? That's what I mean by WTF. You could definitely see the CYA moves coming a mile away.[4]

Following the collapse of Healthcare.gov, the Administration endeavored to keep the true nature of the website's problems out of the public eye. Days after the launch, Administration

[3] Transcribed Interview with Teresa Fryer, Chief Information Security Officer, CMS, in Washington, D.C. (Mar. 26, 2014).

[4] Email from Zac Jiwa, Innovation Fellow, Dep't of Health and Human Services, to Bryan Sivak, Chief Technology Officer, Dep't of Health and Human Services (Nov. 18, 2013 3:14:35 EST). [emphasis added]

officials downplayed the website's problems by blaming the high volume of visitors to the site. However, documents show that high-ranking officials knew that high volume was not the root cause of the website's considerable functionality issues, and acknowledged that the press did not know the full story. When CMS officials learned that account creation figures were leaked to the press, they responded by further restricting access within CMS to the data. CMS officials advised consumers to contact the ObamaCare call centers, despite concerns about their effectiveness. Angry and embarrassed that software developers were bashing Healthcare.gov code on the popular website Github, CMS officials removed the code from public view.

The Administration has repeatedly attempted to obstruct Congressional investigation of the launch of Healthcare.gov. In August 2014, CMS informed the Committee that it had lost emails responsive to the Committee's subpoena of documents relevant to development of Healthcare.gov. CMS Administrator Marilyn Tavenner admitted to deleting her own emails during the time period of ObamaCare implementation. Her actions prevent Congress from conducting effective oversight, and also prevent the public from accessing information under the Freedom of Information Act (FOIA).

Even after the first open enrollment period ended, the obstruction continued. In May 2014, CMS officials stopped releasing monthly updates on the number of ObamaCare enrollees, causing even supporters of the law to question this decision. In August 2014, CMS refused to provide the *Associated Press* documents related to the exchange's security which were requested under FOIA. CMS cited unspecified security concerns which the *Associated Press* pointed out "conflicts with President Obama's promise not to withhold government information over 'speculative or abstract fears."[5] Even more recently, CMS refused to provide to the Government Accountability Office (GAO) documentation related to 13 incidents related to data security. The GAO was conducting an audit of the exchange's privacy and information security controls on behalf of 48 congressional offices.

This Committee's oversight shows multiple troubling instances where ineffective government agencies concealed information about their failures not only from their own colleagues and leaders, but also from the news media, state partners, Congress, and the American people. The examples referenced in this report raise serious concerns about the Administration's transparency and accountability over ObamaCare implementation. As the next open-enrollment period approaches, many questions still remain.

The Administration has already spent a billion dollars on a website that is still not fully operational, and it remains unclear whether the Administration has corrected the many deficiencies that led to the disastrous launch. The same government officials responsible for the lack of transparency and accountability a year ago remain in positions of authority. Administration officials must be held accountable for obstructing public and private access to necessary information, and the Administration must acknowledge that it has failed to live up to President Obama's declaration that he is running the "most transparent administration in history."[6]

[5] Jack Gillum, *US Won't Reveal Records on Health Website Security*, THE ASSOCIATED PRESS (Aug. 19, 2014), *available at*: http://bigstory.ap.org/article/us-wont-reveal-records-health-website-security.
[6] Jonathan Easley, *Obama Says His is the 'Most Transparent Administration in History'*, THE HILL, Feb. 14, 2013.

FINDINGS

Accountability Breakdowns

- HHS officials contemplated a "covert ops mission" to circumvent incompetent CMS officials: **"I grow weary of the bullshit passive/aggressiveness of Henry [Chao], or rather his lack of engagement to the point that we can only speculate that it is passive/aggressiveness. ... The other way to do this is through a complete covert ops mission to unseat the CMS FFE rules engine."**

- CMS refused to share information with HHS officials they felt were not adequately invested in the development of Healthcare.gov. When HHS's Frank Baitman asked CMS's Henry Chao for more visibility into the project, Mr. Chao wrote: **"If you can't recognize a burning house and its implications, what good is it to have a bunch of firemen tell you there's a burning house if you're not going to do anything about it."**

- When HHS employee Julie Herron transferred to CMS before the website's launch, she funneled information about security testing to HHS's Bryan Sivak, who told Ms. Herron **"I don't want to tell anyone that we talk anymore."** Mr. Sivak used Ms. Herron's information about system readiness results to recommend that HHS **"declare victory without fully launching [the website]."**

- CMS official Teresa Fryer acknowledged that that other CMS officials did not properly convey the true state of security testing leading up to the launch: **"Kevin Charest [HHS CISO] has asked for an update of the FFM testing by noon tomorrow and I'm going to give him a truthful update of exactly what is going on. I am tired of the cover ups."**

- When CMS officials were unhappy with the negative results of MITRE's independent security assessment, CMS's Thomas Schankweiler sought to have it changed: **"We need to hit the pause button on this report and have an internal meeting about it later next week. It is important to look at this within the context of the decision memos and ATO memo that is going up for Tony [Trenkle, CMS Chief Information Officer] and Michelle [Snyder, CMS Chief Operating Officer] to sign. ... It is very possible that this report will be reviewed at some point by OIG, and could see the light of day in other ways."**

- After the launch, HHS officials sharply criticized CMS's management leading up to the launch of Healthcare.gov. Referencing an email in which a CMS official admits the system could not handle more than 500 concurrent users, **Mr. Baitman wrote "Frankly, it's worse than I imagined!" and Mr. Sivak replied, "Anyone who has any software experience at all would read that and immediately ask what the fuck you were thinking by launching."**

Transparency Failures

- On October 6, 2013, five days after the website's disastrous launch, Todd Park, a White House official, assured the public that high volume was the reason for the so-called glitches: "These bugs were functions of volume…. Take away the volume and it works." However, high ranking CMS and HHS officials who reported to Mr. Park knew that high volume was not primarily to blame. **Two days after the launch, HHS's Bryan Sivak wrote "This is a fucking disaster. It's 1am and they don't even know what the problem is, for sure. Basic testing should have been done hours ago that hasn't been done." A CMS employee responded, "This is going to turn ugly and someone is going to leak that CMS has no clue about the problem."**

- CMS and HHS officials acknowledged that the public and the press did not know the truth about Healthcare.gov's problems. **A CMS employee wrote, "Politico has a Day 2 story that talks about the issues. Quotes NY as having the 'most detailed' explanation but it's still just stating overwhelming traffic that 'couldn't have been replicated in testing'." Mr. Sivak responded, "1. Bad architecture 2. Not enough testing. Pretty simple really."**

- CMS reduced internal access to user account metrics when the media reported accurate figures, suspecting a leak within CMS. **CMS's Marianne Bowen wrote, "[s]ome of the metrics that are being reported are showing up in newspapers and they're close enough to reality to know someone with knowledge of the metrics is talking."**

- CMS removed Healthcare.gov code from open source project, Github, for public relations reasons because developers were publicly criticizing the code: **"[t]his Github project has turned into a place for programmers to bash our system, submit service requests (!) and now people have started copying Marketplace source code that they can see and making edits to that (!!). ... I am sure there may be some blowback from this decision but I think it is better to take a short term hit with this deletion than to let this bashing of the source code continue on our official Github site on an ongoing basis."**

- In response to draft talking points that noted concerns about the lack of training for consumer representatives at the ObamaCare Call Centers, CMS's Julie Bataille wrote, **"We NEVER want to say most of this publicly. We need consumers to call us and not worry about these details."**

- In violation of federal record-keeping rules, Administrator Tavenner deleted her emails, and instructed subordinates to do so as well. In an email, dated October 5, 2013, Ms. Tavenner forwarded a complaint from Jeanne Lambrew, a key White House advisor, about call center workers giving callers incorrect information: **"Please delete this email –but please see if we can work on call script [redacted]."**

I. INTRODUCTION

Many of Healthcare.gov's failures stem from the Administration's lack of transparency and collaboration within its own agencies. Part II of this report documents counterproductive infighting between officials at the Centers for Medicare and Medicaid Services and their colleagues at the Department of Health and Human Services, as well as factions within CMS, whose tendency to look for others to blame when problems arose contributed to a complete breakdown in accountability within the Administration. Part III explores the Administration's lack of transparency with the news media, independent oversight agencies, state partners, and the American people. Part IV details how the Administration's obstruction continues, as leaders within HHS and CMS escape accountability for their actions.

II. ACCOUNTABILITY BREAKDOWNS

CMS and HHS officials failed to effectively collaborate and communicate during the testing and launch of Healthcare.gov, leading to disastrous outcomes. CMS officials developing the exchange refused to share vital information with senior IT officials at HHS, even while communicating directly with White House officials. Left out of the loop, HHS officials resorted to using informants within CMS to obtain crucial information, often communicating over private email. Furthermore, hostile factions developed within CMS, as competing groups sought to have their opinions heeded. Many administration officials acknowledged that the truth about the state of security testing was obscured by unrealistic timelines and poor communication. These tense relationships resulted in blame-shifting, little collaboration, and ultimately, a complete lack of accountability on the part of officials responsible for the Healthcare.gov debacle.

A. HHS Officials Used Informants to Obtain Information about Healthcare.gov from Secretive CMS Officials.

The relationship between CMS and HHS IT officials deteriorated in the months leading up to the website's launch, as CMS officials refused to share vital information with superiors at HHS, opting instead to communicate directly with White House officials. In January 2013, Frank Baitman, HHS Chief Information Officer (CIO), asked Tony Trenkle, CMS CIO, and Henry Chao, CMS Deputy CIO and a key manager in the development of Healthcare.gov, for greater access to information regarding the development of Healthcare.gov. Mr. Baitman wrote that "[g]iven the importance of this project to the Secretary and the White House, it'll continue to receive very high level attention; thus, we need to ensure that emerging issues – which are inevitable – are effectively understood and analyzed at the appropriate level."[7] Mr. Baitman expressed concerns about "poor information flow between policy, operational and IT planners/developers," and noted that "critical knowledge is concentrated in key personnel at CMS."[8] He recommended that critical project knowledge be "more broadly distributed" and that

[7] Email from Frank Baitman, Chief Information Officer, Dep't Health and Human Services, to Tony Trenkle, Chief Information Officer, CMS, et.al (Jan. 22, 2013) [HHS-0108861,2].
[8] *Id.*

he and Bryan Sivak, HHS Chief Technology Officer (CTO), have more "visibility" into CMS's efforts.[9]

Mr. Chao, citing a conversation he had with United States Chief Technology Officer Todd Park, disagreed with Mr. Baitman's assessment that HHS should be given more visibility into the Healthcare.gov project. Mr. Chao wrote to Mr. Trenkle that "[m]y discussion with Todd just now is sort of the opposite of what Frank [Baitman] is asking for … in order to have the so-called 'visibility' you have to at least in some way understand the complexity and vastness of the undertaking."[10] He continued:

> If you can't recognize a burning house and its implications, what good is it to have a bunch of firemen tell you there's a burning house if you're not going to do anything about it. If you want to know how many houses burned down, how many firemen you have, and how many fire engines you have then we can tell you on a monthly basis, but that would be HHS passively receiving information. If they want to play an active role then they really have to roll up their sleeves, otherwise it'll be just time wasted trying to convey issues and options to a body that is not in position to make the proper calls.[11]

Mr. Chao further questioned whether HHS was as invested in the project as CMS, writing that "[w]ithout that personal investment in establishing the basis for understanding the operational aspects of the program (which HHS clearly does not have), there is no way to have a meaningful dialogue about the issues that 'visibility' provides you."[12]

Poor communication and collaboration between CMS and HHS continued after Mr. Baitman's January 2013 email. On March 18, 2013, HHS employee Zac Jiwa complained to Mr. Sivak about the lack of transparency at CMS's Office of Information Services (OIS). CMS's secrecy created barriers to HHS's attempt to develop a program to calculate modified adjusted gross income, a key figure used to determine an applicant's eligibility for subsidies. Mr. Jiwa wrote:

> [a]t the end of the day, OIS, through its contracts with CGI and QSSI, will have to carry the torch to make this project successful. Chris [Lunt, another HHS employee] nor I can do it alone and unless they have 'marching orders', I don't see them putting the necessary resources behind it. I grow weary of the bullshit passive/aggressiveness of Henry [Chao], or rather his lack of engagement to the point that we can only speculate that it is passive/aggressiveness.[13]

Mr. Jiwa then contemplates going around CMS officials by conducting a "complete covert ops mission to unseat the CMS FFE [federally-facilitated exchange] rules engine."[14] He concludes

---

[9] *Id.*
[10] *Id.*
[11] *Id.* [emphasis added]
[12] *Id.*
[13] Email from Zac Jiwa, Innovation Fellow, Dep't of Health and Human Services, to Bryan Sivak, Chief Technology Officer, Dep't of Health and Human Services (Mar. 18, 2013) [SIVAK_HOGR 000017]. [emphasis added]
[14] *Id.* [emphasis added]

that "As much as I like that idea ... I think we have little chance of pulling off a coup and we do not want to bite off more than we can chew."[15]

In a September 6, 2013, email chain on cyber-security concerns, Mr. Baitman once again reiterated concerns about being kept uninformed about the development of the website. He wrote to Michelle Snyder, CMS Chief Operating Officer:

> One of the challenges I have faced is the lack of vision into the Marketplace development effort since I came onboard – as well as the Marketplace security preparations. We're just getting a copy of the hub ATO [authority to operate], and will begin to review the testing and other documentation over the weekend. The larger issue, as you well know, is with the FFM modules – where I'm told that a code freeze still has not occurred. It's going to be quite a challenge to do user acceptance and security testing, remediation, and regression testing on our timeline.[16]

He then reiterated his offer to assist CMS with "specific resources" and noted that his "offer stands" in the last month leading up to the launch.[17]

In early September 2013, Mr. Baitman arranged for his staff to conduct separate testing of the marketplace during the week of September 22, 2013, on various application scenarios (i.e. types of households, types of tax filers) and common security risks. Mr. Baitman wrote, "[a]s with all large enterprise systems, there are certain to be bugs, dead-ends, or incorrect calculations. I'd like to know about them before we go live the following week!"[18] While it is unclear whether this testing ultimately took place, Mr. Baitman's plans for separate testing indicate not only dysfunctional lines of communication between HHS and CMS, but also inherent suspicion between the two entities. HHS did not trust CMS to inform them fully, and CMS did not trust HHS to give helpful input.

An August 2013 email chain further illustrates the odd relationship between CMS and HHS on the project, as HHS officials began to secretly seek information about the project though informants. Julie Herron, a former subordinate to Mr. Sivak, had been transferred to CMS to work on activities occurring on "Day 2", referring to website components not needed on October 1st, but needed shortly afterwards. Ms. Herron funneled information to Mr. Sivak about the development of Healthcare.gov. For example, she wrote that "Jon, Ketan, & Henry [Chao] are apparently locked in the Command Center (still) working through issues and I suspect that will continue until launch."[19] Mr. Sivak indicated that he wanted to keep communications with Ms.

---

[15] *Id.* [emphasis added]
[16] Email from Frank Baitman, Chief Information Officer, Dep't Health and Human Services, to Michelle Snyder, Chief Operating Officer, CMS (Sept. 6, 2013) [HHS-0103206]. [emphasis added]
[17] *Id.*
[18] Email from Frank Baitman, Chief Information Officer, Dep't Health and Human Services, to Timothy Monteleone, Director, Capital Planning and Investment control, Dep't Health and Human Services, et. al (Sept. 11, 2013) [HHS-0106573].
[19] Email from Julie Herron, Project Manager, Dep't Health and Human Services, to Bryan Sivak, Chief Technology Officer, Dep't of Health and Human Services (Aug. 20, 2013) [SIVAK_HOGR 000280,81].

Herron secret from CMS, writing "I don't want to tell anyone that we talk anymore :)."[20] In reply, Ms. Herron wrote "Good point."[21]

In the same email chain, Ms. Herron informed Mr. Sivak via email that she would probably not have "day-to-day access to the Day 1 work."[22] Mr. Sivak responded, "I don't see how you wouldn't get access to day 1 stuff – how are you supposed to help with day 2 if you don't know what day 1 is? … If you don't get access, I'm probably going to start being a little bit of a dick, which will give you ample opportunity to badmouth me and gain the trust of people at CMS."[23]

On September 10, 2013, Ms. Herron forwarded Mr. Sivak a message from another staff member involved with the project. The email, titled "From Ed" read:

> I don't know who is making the calls about what gets cut and what stays. The relationships between OIS, OC [Office of Communications], and CCIIO are very opaque. CGI seems to have failed to deliver so much that all the timelines and deadlines of the last 8 months seem like a total fiction. It does not surprise me that Bryan [Sivak] has only seen parts. I would be very surprised to hear if there is a working end-to-end version in existence. I have yet to hear of one. So to your question of how I'm feeling about launch…not good. Kind of Heartbroken, actually. Whatever launches, if functional, will only technically meet the criteria of launching the exchange. It will be riddled with confusing and hard-to-use compromises. But I don't really. I'm not seeing anything that's being delivered. I'm just piecing things together through the grapevine.[24]

Mr. Sivak responded, "like I said, it's all negative. I'm going to embark on a campaign to declare victory without fully launching. We'll see."[25] Mr. Sivak testified that on September 10, 2013, he along with Frank Baitman approached HHS leadership about implementing a phased launch of Healthcare.gov, similar to a beta test.[26] Mr. Baitman and Mr. Sivak brought up the idea of a delayed launch at a meeting of HHS leadership including Deputy Secretary, Bill Corr, Director of the HHS Office of Health Reform, Mike Hash, and CMS Administrator, Marilynn Tavenner.[27] However, both testified that their suggestion was rejected.[28]

---

[20] *Id.* [emphasis added]
[21] *Id.*
[22] *Id.*
[23] *Id.* [emphasis added]
[24] Email from Julie Herron, Project Manager, Dep't Health and Human Services, to Bryan Sivak, Chief Technology Officer, Dep't of Health and Human (Sept. 10, 2013). [emphasis added]
[25] *Id*. [emphasis added]
[26] A beta test is "a field test of the beta version of a product (as software) especially by testers outside the company developing it that is conducted prior to commercial release." (*available at:* http://www.merriam-webster.com/dictionary/beta%20test).
[27] Transcribed Interview Franklin Baitman, Chief Information Officer, Dep't Health and Human Services, in Washington, D.C. (Jan. 14, 2014); Transcribed Interview of Bryan Sivak, Chief Technology Officer, Dep't of Health and Human, in Washington, D.C. (Feb. 12, 2014).
[28] *Id.*

After the launch, Mr. Baitman and Mr. Sivak traded emails in which they sharply criticized CMS's management of the project. Mr. Sivak showed Mr. Baitman emails that were made public by Congress in the wake of Healthcare.gov's disastrous launch. In these emails, dated September 27, 2013, a CMS official working on the FFM development, wrote "the facts are that we have not successfully handled more than 500 concurrent users filling out applications in an environment that is similarly in size to Day 1 production."[29] In response, Mr. Baitman wrote "Frankly, it's worse than I imagined!"[30] Mr. Sivak replied, "Anyone who has any software experience at all would read that and immediately ask what the fuck you were thinking by launching."[31] Mr. Baitman answered, "but, and here's the thing, these people DID have software experience! Henry [Chao], Dave [Nelson], and as I understand it, Todd. Not to mention the vendors. The protestations in these files are remarkably muted given the reality."[32]

From the perspectives of Mr. Baitman and Mr. Sivak, CMS made a grave error in judgment by fully launching the website on October 1, 2013, given the problems the project had encountered. They even suggested to HHS leadership that the website launch be limited to a smaller population in order to identify and fix inevitable problems at launch. The breakdown between HHS and CMS is significant, not only because it prevented HHS from fully assisting with its resources and expertise, but also because HHS was not in a position to effectively monitor the project's progress and provide oversight when needed.

Senior Administration officials appear to have had a remarkable lack of interest in the IT progress and accepted positive reports uncritically. This sentiment can be encapsulated in a conversation between Mr. Jiwa and Mr. Sivak in November 2013. Mr. Jiwa wrote:

> Here is what I don't understand. Is there some misunderstood 'understanding' going on here? I mean it is a complete embarrassment for the President to get up and say 'he never knew' that there was problems prior to Oct. 1. Either that is a lie (I don't particularly believe he is a blatant liar) or his staff is not communicating. I mean you [Bryan Sivak] knew it, but your leadership only wanted to hear beautiful music and talk about rainbows and unicorns. Todd [Park] had to have known it, but somehow he had the utmost faith in Henry [Chao] and team. I'm just totally missing how it got to this point. And I don't mean the technical delivery…I mean the out and out incompetence. Unless it is some sort of conspiracy…Maybe the House of Cards is real! But clearly, these people are not smart enough to pull it off. So, yeah, I'm a little confounded. How did one week Henry Chao tell us there was no way Account Transfer would be ready, then a meeting at the White House and a week later, oh, yeah, everything is back on track, we'll meet the dates? That's what I mean by WTF. You could definitely see the CYA moves coming a mile away.[33]

---

[29] House Energy and Commerce Committee, *available at*: http://energycommerce.house.gov/sites/republicans.energycommerce.house.gov/files/20131121-Sept26to30AdministraitonEmails.pdf.

[30] Email from Frank Baitman, Chief Information Officer, Dep't Health and Human Services, to Bryan Sivak Chief Technology Officer, Dep't of Health and Human Services (Nov. 22, 2013) [SIVAK_HOGR 000170]. [emphasis added]

[31] *Id.* [emphasis added]

[32] *Id.* [emphasis added]

[33] Email from Zac Jiwa, Innovation Fellow, Dep't of Health and Human Services, to Bryan Sivak, Chief Technology Officer, Dep't of Health and Human Services (Nov. 18, 2013 3:14:35 EST). [emphasis added]

Ultimately, the Administration bears responsibility for ensuring that an appropriate monitoring framework was in place for the exchange's development.

B. Hostile Factions within CMS Fought About Negative Security Test Results, as Officials Sought to Alter an Unflattering Independent Security Assessment.

Two separate teams within CMS conducted security testing for the federal exchange, also known as the Federally-Facilitated Marketplace. The first team, headed by Thomas Schankweiler, an Information Security Officer at CMS, coordinated the day-to-day security activities of the FFM development, working closely with CMS Deputy CIO Henry Chao and the development team. The second team was run through the Enterprise Information Security Group (EISG) within CMS, headed by Teresa Fryer, the Chief Information Security Officer. EISG's role was to oversee the Security Control Assessment, a key milestone the system would undergo in order to begin operations. Instead of collaborating, documents show significant conflicts between Mr. Schankweiler's FFM development team and Ms. Fryer's EISG team. This counterproductive infighting contributed to poor security testing results and Mr. Schankweiler's scheme to contest negative and embarrassing findings from the independent assessment.

In late September 2013, Ms. Fryer's EISG team tasked The MITRE Corporation, a federally funded research and development firm with expertise in this area, to conduct a security assessment for the FFM. MITRE's role was to provide an independent assessment of the FFM system prior to launch. However, at the time, significant components of the FFM remained unfinished and MITRE faced difficulties in testing the system. Their inability to effectively test the system was a significant concern for both the MITRE testers and Ms. Fryer's EISG team. Because of these concerns, Ms. Fryer testified that she recommended denying the Authority to Operate (ATO) for the FFM, which would prevent the system from launching, due to concerns over problems with security testing.[34] However, other CMS employees disagreed with Ms. Fryer and advocated signing the ATO regardless of security concerns.[35]

Ms. Fryer testified she felt that the daily reports on SCA tests did not fully convey the testing challenges experienced by the security testers.[36] For example, in a September 17, 2013, email, Ms. Fryer wrote: "there were many interruptions affecting testing such as the environment was unstable and EIDM was also down. So not much testing got done."[37] Therefore, despite the fact that there were no security vulnerability "findings" during that day of testing, very little testing was actually performed given the components of the system that were inoperable that day. Ms. Fryer then wrote to Mr. Linares "Kevin Charest [HHS CISO] has asked for an update

[34] Transcribed Interview with Teresa Fryer, Chief Information Security Officer, CMS, in Washington, D.C. (Dec. 17, 2013).
[35] Ordinarily, the Chief Information Officer's signature on an ATO signifies that the federal system was sufficiently tested to be secure, and was ready to go-live. However, due to the problems with the security testing, CMS CIO Tony Trenkle took the unprecedented step of elevating the ATO decision to Administrator Tavenner who authorized the FFM on September 27, 2013.
[36] Transcribed Interview with Teresa Fryer, Chief Information Security Officer, CMS, in Washington, D.C. (Mar. 26, 2014).
[37] Email from Teresa Fryer, Chief Information Security Officer, CMS, to George Linares, Chief Technology Officer, CMS (Sept. 17, 2013) [HHS-0103293].

of the FFM testing by noon tomorrow and I'm going to give him a truthful update of exactly what is going on. I am tired of the cover ups."[38] In a transcribed interview, Ms. Fryer testified: "[O]ur job as security experts is to portray the posture or the events that are happening and to brief senior leadership management on the security issues that are being raised during testing. And I felt that they were not being properly being briefed or properly portrayed, the issues that were happening that week during security testing."[39]

CMS's FFM development team was harshly critical of Ms. Fryer's EISG team in return. For example, on September 17, 2013, Henry Chao criticized MITRE's security testers for conducting "business as usual." He wrote:

> This is not business as usual and I neither have the time nor patience to explain what situation we are in right now. I had hoped the SCA testers would appreciate the intent of the message of dire urgency I gave to them about wrapping up testing as early as possible, including starting on Monday, but they followed their usual procedure and did not start early until they met with all the people and got all the demos. In other words they paid no attention to me to not treat this as business as usual. If they would have started earlier and not Cut [sic] out at 5pm maybe they wouldn't be saying they don't have enough time.[40]

Chao concluded, "Security testing is of utmost importance but it is just one factor to balance among multiple factors to meet the implementation date so I appreciate any support I can get on this front." Ms. Fryer forwarded Mr. Chao's email to George Linares, CMS CTO, writing, "I am not going to continue with the bullshit email conversation with Henry."[41] Ms. Fryer then rebutted Mr. Chao's criticisms and blamed the FFM development team for the delayed timeline: "the environment wasn't available for testing on Monday" and that the hours available for security testing were "dictated by CIISG [Consumer Information and Insurance Group, the CMS group responsible for developing the exchange] and CGI."[42]

Once MITRE completed their September Security Assessment, Mr. Schankweiler's FFM development team was unhappy with the report and sought to have it changed. On September 26, 2013, Darren Lyles, one of the IT security officials assigned to the FFM development team, wrote Ms. Fryer:

> The Draft SCA [security control assessment] Report has been called into question by CGI [primary contractor building the FFM] and CIISG [Consumer Information Insurance Group, the team within CMS that works with contractors to develop the FFM and other Healthcare.gov components] Stakeholders. There are assertions made in the report that are deemed to be erroneous and misrepresentative of what

[38] *Id*. [emphasis added]
[39] Transcribed Interview with Teresa Fryer, Chief Information Security Officer, CMS, in Washington, D.C. (Mar. 26, 2014).
[40] Email from Henry Chao, Deputy Director of the Office of Information Services, CMS, to Teresa Fryer, Chief Information Security Officer, CMS, et. Al. (Sept. 17, 2013) [HHS-013293].
[41] *Id.*
[42] *Id*.

actually occurred. I have attached the report that has been commented on by CGI and would like to submit this for your review."[43]

Michael Mellor, Ms. Fryer's deputy, responded to Mr. Lyles: "Keep in mind – that the purpose of the SCA is to provide an independent assessment of the security posture of a system. As part of that independent assessment, the maintainer of the system likely will not agree with all of the findings and the SCA report."[44]

Mr. Schankweiler, Mr. Lyles' superior, then responded to Mr. Mellor, insisting that the report should be reviewed by senior CMS officials and worried the report would be seen by others outside CMS: "We need to hit the pause button on this report and have an internal meeting about it later next week. It is important to look at this within the context of the decision memos and ATO memo that is going up for Tony [Trenkle, CMS Chief Information Officer] and Michelle [Snyder, CMS Chief Operating Officer] to sign."[45] Mr. Schankweiler then wrote the report was "only partially accurate, and extremely opinionated, false, misrepresentative, and inflammatory." Mr. Schankweiller noted that "It is very possible that this report will be reviewed at some point by OIG, and could see the light of day in other ways."[46] Mr. Schankweiler offered to "look at the report from the government perspective and provide ... analysis."[47]

On October 7, 2013, the lead security tester for MITRE, Milton Shomo, wrote Jane Kim, a CMS official on Ms. Fryer's EISG team, "CCIIO [Centers for Consumer Information and Insurance Oversight, one of the divisions at CMS responsible for running the exchange] and CGI Federal had some issues with some of the information in our Marketplace … draft SCA report from the assessment we did in August and September. MITRE stands behind everything in our report as an accurate description of the assessment. I would like to be able to deliver the final report and book package as soon as we can so hopefully there will not be too much delay in getting us the word to produce the final report."[48] Ms. Kim responded that the EISG team, unlike the FFM development team, "considered the report done last week" and that they "basically agreed with all of MITRE's comments."[49]

Mr. Shomo later wrote to Ms. Kim, "My feeling is that CCIIO is dragging their feet on saying go ahead with the final report since they were somewhat unhappy with the draft report."[50] On October 9, 2013, Ms. Kim informed Ms. Fryer that "Darren [Lyles] still has not gotten back

---

[43] Email from Darren Lyles, to Teresa Fryer, Chief Information Security Officer, CMS (Sept. 26, 2013) [HHS-0017249]. [emphasis added]
[44] Email from Michael Mellor, Deputy Chief Information Security Officer, CMS, to Darrin Lyles, Information System Security Officer, CMS (Sept. 27, 2013). [emphasis in original]
[45] Email from Thomas Schankweiler, Security Officer, CMS, to Michael Mellor, Deputy Chief Information Security Officer, et. al. (Sept. 27, 2013). [emphasis added]
[46] *Id.*
[47] *Id.* [emphasis added]
[48] Email from Milton Shomo, Principal Information Systems Engineer, MITRE Corp., to Jane Kim, Office of Administrator, CMS (Oct. 7, 201, 4:06 EST). [emphasis added]
[49] Email from Jane Kim, Office of Administrator, CMS, to Milton Shomo, Principal Information Systems Engineer, MITRE Corp., (Oct. 7, 201, 4:27 EST).
[50] Email from Milton Shomo, Principal Information Systems Engineer, MITRE Corp., to Jane Kim, Office of Administrator, CMS (Oct. 7, 201, 4:36 EST).

to Jim [Bielski, MITRE tester]. At this point, I consider our draft the draft report. We've taken the legitimate concerns into account."[51]

Independent security testing is a key aspect in a systems oversight. Documents reviewed by the Committee show conflicts between those responsible for building the exchange and those responsible for assessing the system's security. MITRE testers were forced to conduct their assessment while other developers were still making changes to the system and this arrangement lead to numerous conflicts. Finally, when MITRE issued a draft report, CMS officials developing the exchange were unhappy with the results and inappropriately sought to alter the report in their favor. While there is a role for the project owners to provide feedback, security control assessments must remain fully independent from government influence to produce the desired effect: an unbiased look at the security risks inherent in the system.

III. TRANSPARENCY FAILURES

In the wake of Healthcare.gov's disastrous launch, CMS and HHS acted to obscure the full extent of the problem from public view. Despite public assurances that the website's numerous functionality errors were due to a "high volume" of users on the site, documents show that high-ranking officials knew that was not the case. To prevent more public criticism, CMS officials narrowed employee access to account user statistics in fear that accurate numbers had leaked to the press, agreed to conceal problems with call centers from the public, and removed Healthcare.gov code from an open source project intended to foster collaboration.

Recently, Administrator Tavenner informed the Committee that, in violation of federal record-keeping rules, she inappropriately deleted some of her emails that may have been responsive to Congressional inquiry. CMS's lack of transparency extended to state partners as well. When the Idaho Exchange Board requested a copy of the FFM Authority to Operate, CMS officials contemplated backdating a new document to present as the ATO instead of the true document. These examples illustrate how CMS has been hostile to transparency interests, and has hindered a full understanding of the Administration's actions during the implementation of ObamaCare.

A. High-Ranking CMS and HHS Officials Acknowledge the Public was Misinformed about Healthcare.gov's Problems after the Launch.

The high-profile, error-ridden launch of Healthcare.gov attracted significant attention from both the public and the press. Administration officials assured the public that the website was designed to handle 50,000 to 60,000 simultaneous users and that higher than expected volume caused the website to be unusable. For example, on October 6, 2013, five days after the website's launch, Todd Park told USA Today that the "bugs" causing the website to be

[51] Email from Jane Kim, Office of Administrator, CMS, to Teresa Fryer, Chief Information Security Officer, CMS (Oct. 9, 2013).

dysfunctional were entirely due to the large quantities of users visiting the site: "These bugs were functions of volume…. Take away the volume and it works."[52]

Despite their public stance, CMS decision-makers knew that the problems with Healthcare.gov were far more complicated and far-reaching than high volume, and that fixing the so-called "glitches" would be a significant and time-consuming task. Documents obtained by the Committee show that Mr. Park's assertion that Healthcare.gov could function properly with 50,000 to 60,000 users was false. On September 25, 2013, six days before the launch, Monique Outerbridge, one of CMS's primary managers on the FFM project, emailed CMS Chief Information Officer Tony Trenkle about the latest results of the performance tests. She wrote, "We just found out Healthcare.gov can only handle 10,000 concurrent users. Performance testing results in the toilet."[53] Mr. Trenkle responded, "ugh."[54]

In the days immediately following the launch, an email exchange between HHS CTO Bryan Sivak, and Julie Herron, a former employee of his who had transferred to CMS to work on the website launch, confirmed that volume was not the sole reason for the website's problems. In the email chain dated October 3, 2013, Mr. Sivak wrote that "This is a fucking disaster. It's 1am and they don't even know what the problem is, for sure. Basic testing should have been done hours ago that hasn't been done."[55] Ms. Herron responded, "This is going to turn ugly and someone is going to leak that CMS has no clue about the problem."[56] She then commented about Healthcare.gov:

> So basically effed from the start. Which means there must have been only the most basic of tests otherwise someone would have caught it. Or they knew and just crossed their fingers and hoped for the best. Politico has a Day 2 story that talks about the issues. Quotes NY as having the 'most detailed' explanation but it's still just stating overwhelming traffic that 'couldn't have been replicated in testing'.[57]

Mr. Sivak responded, "1. Bad architecture 2. Not enough testing. Pretty simple really."[58]

In her email to Mr. Sivak, Ms. Herron noted that even the "most detailed" explanation coming from the Administration was inaccurate and feared that someone would "leak" that CMS did not even know what went wrong. Later that night, Mr. Sivak updated Ms. Herron that contractors "tweaked" some elements of the website, but they are "shooting in the dark. … They haven't identified the root cause."[59]

---

[52] Tim Mullaney, *Obama adviser: Demand overwhelmed HealthCare.gov,* USA TODAY, Oct. 6, 2013.
[53] Email between Monique Outerbridge and Tony Trenkle (Sept. 25, 2013) [HHS-0110879].
[54] *Id*. [emphasis added]
[55] Email from Bryan Sivak, Chief Technology Officer, Dep't of Health and Human Services to Julie Herron, Project Manager, Dep't Health and Human Services (Oct. 3, 2013) [SIVAK_HOGR 000038-000040]. [emphasis added]
[56] *Id.* [emphasis added]
[57] *Id.* [emphasis added]
[58] *Id.* [emphasis added]
[59] *Id.*

CMS's confusion over Healthcare.gov's capacity problems continued long after the disastrous October 1st launch. On October 13, 2013, Henry Chao emailed his team that Administrator Tavenner had asked him "[h]ow many users can the system handle?" Mr. Chao, requesting help, wrote "[g]iven the behavior of the production environment I am at a loss as to how to answer that question."[60]

B. CMS Engaged in Schemes to Conceal Vital Information from the Public.

Internal emails obtained by the Committee show that CMS and HHS personnel actively engaged in efforts to obscure the truth about Healthcare.gov's significant problems from the news media and the public. CMS officials encouraged consumers to sign up via call centers when the website was unworkable, but emphatically agreed that CMS should not tell consumers there were operational problems with call centers as well. When CMS found that the media had reported accurate account user creation figures, they immediately suspected a leak within CMS and further restricted access to the figures. Finally, despite posting portions of the Healthcare.gov source code on the website Github, initially intended to encourage improvement and collaboration between CMS and web developers, CMS decided to remove the code when developers started to criticize the code.

CMS Officials Agreed to Conceal Problems with Call Centers from Public

In the days after the immediate launch, CMS scrambled to use alternate methods for enrollment, since the website was essentially unworkable for consumers. One version of talking points, drafted by CMS Communications staff on October 5, 2013, gave a detailed explanation for how consumers could enroll on the federal exchange: online, through the call center and via paper application.[61] The talking points explained how the call centers could enroll consumers in place of the unworkable website, noted that paper applications were the least desirable option because they would take longer to process, and cautioned that there would still be some problems with CMS's alternate plan to enroll consumers.[62] For example, the talking points warned that "While all CSRs [customer service representatives] should have been trained to date, there is the possibility that some continue to direct callers to Healthcare.gov to create accounts. CSRs have also been directed to revert to PDF when the on-line tool is not available."[63] Also, the talking points noted that applying via paper application "adds time" for the determination of subsidy eligibility.[64]

In response to the draft talking points, Mary Wallace from the CMS Office of Communications asked "Who is the audience? Is this for public or just up the chain

---

[60] Email from Henry Chao, Deputy Director of the Office of Information Services, CMS, to Keith Rubin, et. al. (Oct. 13, 2013) [HHS-0021259]. [emphasis added]
[61] Email from Aryana Khalid, Chief of Staff, CMS, to Mary Wallace, Deputy Director of the Office of Communications, CMS (Oct. 6, 2013) [HHS-0135925,26].
[62] *Id.*
[63] *Id.*
[64] *Id.*

explanation?"[65] Aryana Khalid, Marilyn Tavenner's Chief of Staff, replied, "[u]p the chain at WH. Not public. I want to get it right and put it to bed. They are annoying :)."[66] In response, Ms. Wallace wrote, "I don't think we ever want to explain this way to the public. That's why I was asking."[67] Julie Bataille, Director of the CMS Office of Communications chimed in, "[t]otally agree. We NEVER want to say most of this publicly. We need consumers to call us and not worry about these details. Reality is that we will need to go back and forth in the background operationally as needs arise. And I think they want to know you can apply and enrolle [sic] at the call center."[68]

However, throughout October, call centers continued to experience significant problems. CNN reported that "In the first days, half of the calls to the phone center had problems, paper applications could not be processed…"[69] Furthermore, an October 3rd document acknowledged widespread problems with the call center.[70] CMS decided to encourage the public to apply through call centers even when CMS knew that there were serious problems, such as lack of training for customer service representatives and delayed processing system for paper applications.

CMS Feared Accurate User Account Statistics Would Leak to the Press

In addition to keeping valuable information about enrollment problems from consumers, CMS officials tightly controlled access to statistics about user accounts in the days after the launch, preventing much of it from becoming public. CMS's Enterprise Identity Management System (EIDM) controls user accounts for Healthcare.gov, and EIDM statistics would record and report how many users set up accounts through Healthcare.gov. In an October 12, 2013, email, Marianne Bowen of CMS Office of the Administrator informed other CMS officials that someone within CMS had shared EIDM user account creation statistics with the press. Ms. Bowen noted that she was responsible for "pulling together metrics for the Administrator, the White House staff and this week the President related to EIDM account set up," and that QSSI, a federal contractor, updated her every hour with new metrics.[71] Ms. Bowen wrote "[s]ome of the metrics that are being reported are showing up in newspapers and they're close enough to reality to know someone with knowledge of the metrics is talking."[72] She continued: "The Administrator and Michelle [Snyder, CMS COO] have asked me to see if I can limit the CMS exposure to this information ... there are lots of CMS staff on those notes [from QSSI] that

[65] *Id.*
[66] *Id.*
[67] Email from Julie Bataille, Deputy Director of the Office of Communications, CMS, to Mary Wallace, Deputy Director of the Office of Communications, et. al. (Oct. 6, 2013) [HHS-0135925,26].
[68] *Id.* [emphasis added]
[69] Lisa Desjardins, *Documents show first days of Obamacare rollout worse than initially realized,* CNN, Nov. 6, 2013, http://politicalticker.blogs.cnn.com/2013/11/06/documents-show-first-days-of-obamacare-rollout-worse-than-initially-realized/.
[70] *Id.*
[71] Email from Marianne Bowen, Office of the administrator, CMS, to Marc Richardson, Director, Division of Healthcare Information Systems, CMS, et. al (Oct. 12, 2013) [HHS-0103728].
[72] *Id.* [emphasis added]

frankly don't appear to need to know this info."[73] She then asked to remove "any but the most critical CMS staff" from the hourly updates, and to "please keep the metrics close."[74]

CMS Removed Healthcare.gov Code from Open Source Website in Response to Criticism

In an April blog post, HHS touted the openness of their website, writing "everything HHS does will be published on GitHub. GitHub is an open source code repository developers can use to share and collaborate on projects."[75] In June, 2013, CMS posted code for some portions of Healthcare.gov, primarily parts of the website that provided information to the public, onto Github.

Mr. Sivak testified that posting source code on Github was a "valuable exercise" because it "leverag[ed] the whole idea is that if you can post the code and there is something that could be done better or improved, then somebody out there in the community can help you make it better and improve it."[76] For example, he explained how Github could be used to strengthen a program's security:

> One of the best ways to ensure the security of any given piece of code is to publish the source code because you have legions of experts out there who can review it and point out any flaws in the code and/or any flaws in the programming that would introduce security risks. Many eyes can solve problems like that; whereas, you know, if you keep things internally, you are never, you know, really guaranteed that all -- you know, enough people are going to be looking at something to spot any issues. It is one of the basic tenets of open source code.[77]

However, on October 11, 2013, CMS employee Jon Booth, complained to top CMS officials including Administrator Tavenner and Mr. Chao, that "this Github project has turned into a place for programmers to bash our system."[78] He recommended that CMS remove the code from Github and noted that, "I am sure there may be some blowback from this decision but I think it is better to take a short term hit with this deletion than to let this bashing of the source code continue on our official Github site on an ongoing basis."[79]

In internal discussions, CMS officials stated two reasons for removing the code: the "bad PR" associated with the online Github discussions and the feeling that it would be a "real or perceived security risk."[80] This shows a lack of understanding of how the internet works. As Mr. Sivak testified, once the source code was posted it could never be erased: "It was nearly 100

---

[73] *Id.*
[74] *Id.*
[75] David Cole, *New Healthcare.gov is Open, CMS-Free,* Apr. 10, 2013, http://www.hhs.gov/digitalstrategy/blog/2013/04/new-heathcare-open-cms-free.html.
[76] Transcribed Interview of Bryan Sivak, Chief Technology Officer, Dep't of Health and Human, in Washington, D.C. (Feb. 12, 2014).
[77] *Id.* [emphasis added]
[78] Email from Jon Booth, Director, Website & New Media Group, CMS, to Marilyn Tavenner, Administrator, CMS, et. al. (Oct. 11, 2013) [HHS-0021188,89,90]. [emphasis added]
[79] *Id.* [emphasis added]
[80] *Id.*

percent certainty that once the repository was deleted, somebody would have reposted it."[81] It is unlikely that CMS's concern for website security motivated the decision to remove the code, partly because it was already publicly available for reposting, and also because the publicly released code did not handle parts of the website that dealt with personal information.

Although Mr. Booth described Mr. Sivak as the "champion" of the idea to post the source code on Github, CMS decided to remove the code without consulting Mr. Sivak and others at HHS.[82] Mr. Sivak testified that, in response to his questions, Ms. Bataille, Director of the CMS Office of Communications, told him the code was removed because CMS was concerned about the publicity the source code was getting and that CMS was afraid the public misunderstood the nature of the code.[83] Mr. Sivak testified that he would have recommended against removing the code because of the benefits that continued collaboration with the developer community would bring, and also that the code would simply be reposted by someone else once it was deleted by CMS anyway.[84]

C. Administrator Tavenner Deleted Emails, Violating Federal Record Keeping Laws and Impeding Oversight.

On October 10, 2013, Chairman Issa and Senate Health, Education, Labor and Pension Committee Ranking Member Lamar Alexander wrote to Secretary Sebelius, requesting documents related to the launch of Healthcare.gov. Due to the Administration's refusal to voluntarily provide documents responsive to the request, the Committee was forced to issue a subpoena on October 30, 2013. On August 7, 2014, more than nine months after the subpoena was issued, CMS informed the Committee that "some of Ms. Tavenner's potentially responsive emails might not be retrievable."[85]

According to a letter to the National Archives, Administrator Tavenner, had "copied or forwarded emails to immediate staff for retention and retrieval, and did not maintain her own copies." However, this practice was not followed consistently and some emails were lost as a result. While some responsive emails sent within HHS might be retrievable, CMS admitted that "[w]hile we have not identified any specific emails that we will be unable to retrieve, it is possible that some emails may not be available to HHS."[86]

Not only did the Administrator's actions prevent responsive documents from being produced for Congressional oversight, but it also restricted private citizens, the press or good government organizations from accessing documents on this and other issues affecting CMS over that time period through the Freedom of Information Act. As Freedom of Information Act

---

[81] Transcribed Interview with Bryan Sivak, Chief Technology Officer, Dep't of Health and Human, in Washington, D.C (Feb. 12, 2014).
[82] Email from Jon Booth, Director, Website & New Media Group, CMS, to Marilyn Tavenner, Administrator, CMS, et. al. (Oct. 11, 2013) [HHS-0021188,89,90].
[83] Transcribed Interview of Bryan Sivak, Chief Technology Officer, Dep't of Health & Human, in Washington, D.C. (Feb. 12, 2014).
[84] *Id.*
[85] Letter from Jim R. Equea, Assistant Secretary for Legislation, Dep't Health & Human Services, to Rep. Darrell Issa, Chairman, H. Comm. on Oversight and Government Reform (Aug. 7, 2014).
[86] *Id.*

expert and *Washington Examiner* editor Mark Tapscott explains, "reports and other official documents, emails, telephone text messages and instant messages on government business are required to be preserved by federal record-keeping regulations… for historical purposes and because they are accessible under the Freedom of Information Act."[87]

Equally troubling is an email sent to Ms. Bataille, Director of CMS Office of Communications. In an email, dated October 5, 2013, Ms. Tavenner forwarded a complaint from Jeanne Lambrew, a key White House advisor, about call center workers giving callers incorrect information. Ms. Tavenner wrote to Ms. Bataille "Please delete this email –but please see if we can work on call script [redacted]."[88] It is unclear whether Ms. Tavenner similarly instructed other officials to delete emails from White House advisors that were forwarded to them. Given CMS's sloppy record handling official documents, it is impossible to know for sure.

D. CMS Officials Suggest Backdating Documents in Response to State Partner's Request for Security Verification Documents.

CMS's lack of transparency extended to communications with their state partners as well. On September 30, 2013, the Idaho Exchange Board requested that CMS provide them information about the federal exchange's "security assessment" in advance of a meeting during which the Board would vote on whether or not to allow the federally-facilitated marketplace to open in their state on October 1st. A CMS employee explained: "Basically, they would like to know if we have access to any of the privacy/security assessments that have been done on the FDSH [Federal Data Services Hub] whether they be internal or external reviews."[89]

Andrea Greene-Horace, a CMS CCIIO employee, explained the Board's request in further detail in an email to Mr. Schankweiler, the FFM's Information Security Officer and others. Ms. Greene-Horace wrote:

> The board members want the 'authority to operate' and want us to provide a link to the FFM's 'Authority to Operate.' They read the Office of the IG's initial review but cannot find a [sic] 'Authority to Connect' or an 'Authority to Operate' for the FFM…They would rather have the document. Please advise on your approach in case we get more requests.[90]

An Authority to Operate is a certification that a system has undergone an independent risk assessment and meets the requirements to launch. Typically, an agency's Chief Information Officer signs the ATO, but in this case, CMS CIO Tony Trenkle refused to sign it because of his concerns about MITRE's security testing results.[91] Instead, he took an unprecedented step by

---

[87] Mark Tapscott, *Mailyn Tavenner's deleted emails pose wuestion: Is the FOIA the law federal officials break most often?,* Aug. 19, 2014, http://washingtonexaminer.com/marilyn-tavenners-deleted-emails-pose-question-is-the-foia-the-law-federal-officials-break-most-often/article/2552153. [emphasis added]

[88] Email from Marilyn Tavenner, Administrator, Dep't of Health and Human Services, to Julie Bataille, Director of Office of Communications, CMS (Oct. 5, 2013) [HHS-0134965].

[89] Email between CMS employees (Sept. 30, 2013) [HHS-0018435, 36].

[90] *Id*.

[91] Transcribed Interview with Tony Trenkle, Chief Information Officer, CMS, in Washington, D.C (Dec. 4, 2013).

asking CMS Administrator Marilyn Tavenner to sign the ATO.[92] During transcribed interviews, no CMS official interviewed by the Committee could recall another instance in which the Administrator, instead of the CIO, authorized a system to go-live.[93]

That afternoon, Mr. Schankweiler, an Information Security Officer at CMS, spoke by phone to the Idaho Exchange Board.[94] Mr. Schankweiler showed the Board the ATO for the Data Services Hub, the component that connects the exchange with state and federal agencies. However, Mr. Schankweiler refused to share the decision memo authorizing the FFM to go-live, arguing that it was "sensitive."[95] In fact, Mr. Schankweiler's testimony was required only because CMS could not provide an ATO for the FFM. Based on Schankweiler's testimony, the Board voted to proceed with the launch of YourIdahoHealth.org, without the requested documentation from CMS.[96] However, Board members expressed continued reservations about the lack of documentation.[97]

After Mr. Schankweiler spoke with the Board by teleconference, he reported back to his colleagues that they "do have one action regarding the request for follow up document to support the verbal attestation provided during [the call] ... They are now looking for document of the ATO memo for the FFM."[98] Mr. Schankweiler noted that the Board and others were "looking for the normal ATO package, with the Decision Memo standing behind it accepting the risk. There is a standard ATO memo that should be created for this. The OIG, Congress, and now the states are looking for this ATO memo. We likely will want to present that with the Decision Memo backing it up."[99]

George Linares, then-Acting CTO for CMS, concerned about requests from external parties to review the FFM's security documentation, wrote: "So in the case that external parties ask to see the FFM ATO, we need to have the standard ATO form available."[100] Mr. Linares then suggested creating a standard-looking ATO form, backdated to the date of the Decision Memo so that this document would appear to be the document certifying the exchange to go-live on October 1, even though that document did not exist.[101] Mr. Linares wrote "I am just concerned with states asking to see the ATO letter and only having the Decision Memo to show."[102] Ultimately, this backdated document was not created.

---

[92] *Id*.
[93] Transcribed Interview with Teresa Fryer, Chief Information Security Officer, CMS, in Washington, D.C. (Dec. 17, 2013); Transcribed Interview with Tony Trenkle, Chief Information Officer, CMS, in Washington, D.C (Dec. 4, 2013); Transcribed Interview with Kevin Charest, Chief Information Security Officer, Dep't Health and Human Services, in Washington, D.C. (Jan. 8, 2014); Transcribed Interview, George Linares, Chief Technology Officer, CMS, in Washington, D.C. (Jan. 10, 2014); Transcribed Interview Franklin Baitman, Chief Information Officer, Dep't Health and Human Services, in Washington, D.C. (Jan. 14, 2014).
[94] Austin Hill, *Idaho insurance exchange votes to press forward despite concerns about data security*, IDAHO REPORTER (Sept. 30, 2013).
[95] *Id*.
[96] *Id*.
[97] *Id*.
[98] CMS email (Sept. 30, 2013) [HHS-0018433, HHS-0018434].
[99] CMS email (Sept. 30, 2013) [HHS-0018451]. [emphasis added]
[100] *Id*.
[101] *Id*.
[102] *Id*.

The discussion about backdating the ATO demonstrates that CMS officials were aware of the non-standard process used to issue the FFM ATO and considered the FFM decision memo as "sensitive." They acknowledged that if outside entities such as Congress, GAO, and the IG reviewed the memo, it would lead to additional questions on the FFM's security. To avoid that, they contemplated steps to make this memo look more legitimate.

IV. OBSTRUCTION CONTINUES AS THE ADMINISTRATION FAILS TO HOLD LEADERS ACCOUNTABLE FOR TRANSPARENCY FAILURES

Despite numerous complaints about the Administration's pattern of deception throughout ObamaCare implementation, Administration officials continue to obstruct the news media, independent oversight agencies, and congressional investigators, and conceal important information from the American public to protect their political interests. In August 2014, CMS refused to disclose federal records about the security of Healthcare.gov as requested by the *Associated Press* under the Freedom of Information Act.[103] In May 2014, the Administration stopped releasing monthly updates on ObamaCare enrollment figures, without providing any justification.[104] The Government Accountability Office informed the Committee in a briefing that CMS refused to provide GAO with reports of 13 Healthcare.gov "security incidents," even though the GAO was conducting an audit of efforts taken by CMS to ensure the site's security.[105] Officials must be held accountable for obstructing access to necessary information, and the Administration must acknowledge that it has failed to live up to President Obama's declaration that he is running the "most transparent administration in history."[106]

HHS Refused to Provide Documents Requested by the Associated Press *Under Freedom of Information Act*

In late 2013, the *Associated Press* submitted a Freedom of Information Act request for federal records regarding the security of Healthcare.gov, such as the kinds of security software and computer systems behind the federally-funded system.[107] The *Associated Press* requested the records amid concerns that the website was not secure and presented threats to personally identifiable information. However, on August 19, 2014, the Administration denied the *Associated Press* access to the documents.[108] A CMS spokesperson stated that the release of the documents "would potentially cause an unwarranted risk to consumers' private information."[109]

However, as the *Associated Press* pointed out, "the government, in its denial of the AP request, speculates that disclosing the records could possibly, but not assuredly or even probably,

---

[103] Jack Gillum, *US Won't Reveal Records on Health Website Security*, THE ASSOCIATED PRESS (Aug. 19, 2014), *available at*: http://bigstory.ap.org/article/us-wont-reveal-records-health-website-security.
[104] Kyle Cheney, *Administration Stops Monthly ACA Enrollment Reports*, POLITICO PRO (May 21, 2014).
[105] GAO Briefing with Committee staff (Aug. 27, 2014).
[106] Easley, *supra* note 6.
[107] Gillum, *supra* note 103.
[108] *Id.*
[109] *Id.*

give hackers the keys they need to intrude" which conflicts with President Obama's promise not to withhold government information over "speculative or abstract fears."[110] The *Associated Press* also quotes industry consultant David Kennedy, who testified before the Science and Technology Committee last year, as saying "Security practices aren't private information."[111] This appears to be yet another example of the Administration obstructing oversight in order to prevent public criticism in an election year. The Associated Press has asked CMS to reconsider the decision, but to date, CMS has refused to provide even redacted documents.

The Administration Stopped Releasing Monthly Updates on ObamaCare Enrollment Figures

Another example of the Administration's continued hostility to transparency is the decision to halt the release of monthly reports on ObamaCare enrollment figures. Although HHS had issued monthly reports on enrollment numbers throughout the open enrollment period, in May 2014, the Administration stopped issuing the monthly updates, which *Politico* described as a "major pipeline of information about the impact of the health law heading into the 2014 campaign season."[112] According to an administration spokesman, "HHS issued monthly enrollment reports during the first marketplace open enrollment period in order to provide the best understanding of enrollment activities as it was taking place. ... Now that this time period has ended, we will look at future opportunities to share information about the marketplace that is reliable and accurate over time as further analysis can be done but we do not anticipate monthly reports."[113]

HHS refused to provide a reason for their decision to stop releasing the reports, which had helped policymakers assess benchmarks in President Obama's hallmark program. According to *Politico*, the agency offered no information about the timing or level of detail in any future updates.[114] HHS's decision to stop updating the public on enrollment figures sparked outrage among both ObamaCare supporters and critics. Prominent ObamaCare supporter Charles Gaba, the blogger behind acasignups.net, wrote that "HHS has lost their mind and will deserve every bit of criticism that they receive over it."[115] He added, "The ACA is the Obama administration's single most important policy. Whether you support or oppose it, you have to admit that the ACA has a significant impact on the rest of the economy and many other aspects of American society. ... However, for the remainder of President Obama's term in office, at least, they should absolutely continue to issue monthly reports even during the 'off season.'"[116] An August 27, 2014, letter by U.S. Senators John Barrasso and Lamar Alexander requested updated enrollment figures, noting that the Administration has not released information on exchange enrollment since May.[117]

---

[110] *Id.*
[111] *Id.*
[112] Cheney, *supra* note 104.
[113] *Id.*
[114] *Id.*
[115] Charles Gaba, *HHS To Stop Issuing Monthly Reports*, May 21, 2014, http://acasignups.net/14/05/21/hhs-stop-issuing-monthly-reports.
[116] *Id.*
[117] Liz Wolgemuth, *Barrasso, Alexander: Americans Deserve to See New, Accurate Obamacare Enrollment Date,* Aug. 27, 2014, http://www.help.senate.gov/newsroom/press/release/?id=7efd4ccd-45eb-440f-ad76-b5a77cf5be09.

The Administration Refused to Provide the Government Accountability Office with Requested Information

In addition to obstructing policy makers and congressional investigators by refusing to make enrollment figures public, the Administration stonewalled the Government Accountability Office during a recent audit on the security of the Healthcare.gov website. Forty-eight congressional offices requested that GAO, an independent, non-partisan agency, conduct an audit of the security mechanisms CMS put in place to protect personally identifiable information through Healthcare.gov.

In the course of this audit, GAO requested to review reports for 13 "security incidents" that CMS reported had occurred to Healthcare.gov. When GAO briefed Congressional staff about the report, they revealed that CMS refused to provide copies of the reports.[118] After several requests by GAO, CMS provided a one paragraph summary, stating that none of the incidents resulted in a successful hack.[119] However, GAO was unable to draw conclusions without the actual incident reports, which CMS has refused to provide.[120]

V. CONCLUSION

The Committee's oversight shows multiple troubling instances where ineffective government agencies concealed information about failures that led to the disastrous launch of Healthcare.gov not only from their own colleagues and leaders, but also from the news media, state partners, Congress, and the American people. The examples referenced in this report raise serious concerns about Administration's transparency and accountability. As we enter into the next open-enrollment period, many questions still remain.

The Administration has already spent a billion dollars on a website that is still not fully operational, and it remains unclear whether the Administration has corrected the many deficiencies that led to the disastrous launch. The same government officials responsible for the lack of transparency and accountability remain in positions of authority. Administration officials must be held accountable for obstructing public and private access to necessary information, and the Administration must acknowledge that it has failed to live up to President Obama's declaration that he is running the "most transparent administration in history."[121]

[118] GAO Briefing with Committee staff (Aug. 27, 2014).
[119] *Id*.
[120] *Id*.
[121] Easley, *supra* note 6.