HHS' OWN SECURITY CONCERNS ABOUT HEALTHCARE.GOV

HEARING

BEFORE THE

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED THIRTEENTH CONGRESS

SECOND SESSION

JANUARY 16, 2014

Serial No. 113–94

Printed for the use of the Committee on Oversight and Government Reform

Available via the World Wide Web: http://www.fdsys.gov
http://www.house.gov/reform

U.S. GOVERNMENT PRINTING OFFICE

87–352 PDF WASHINGTON : 2014

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

DARRELL E. ISSA, California, *Chairman*

JOHN L. MICA, Florida
MICHAEL R. TURNER, Ohio
JOHN J. DUNCAN, JR., Tennessee
PATRICK T. MCHENRY, North Carolina
JIM JORDAN, Ohio
JASON CHAFFETZ, Utah
TIM WALBERG, Michigan
JAMES LANKFORD, Oklahoma
JUSTIN AMASH, Michigan
PAUL A. GOSAR, Arizona
PATRICK MEEHAN, Pennsylvania
SCOTT DESJARLAIS, Tennessee
TREY GOWDY, South Carolina
BLAKE FARENTHOLD, Texas
DOC HASTINGS, Washington
CYNTHIA M. LUMMIS, Wyoming
ROB WOODALL, Georgia
THOMAS MASSIE, Kentucky
DOUG COLLINS, Georgia
MARK MEADOWS, North Carolina
KERRY L. BENTIVOLIO, Michigan
RON DESANTIS, Florida

ELIJAH E. CUMMINGS, Maryland, *Ranking Minority Member*
CAROLYN B. MALONEY, New York
ELEANOR HOLMES NORTON, District of Columbia
JOHN F. TIERNEY, Massachusetts
WM. LACY CLAY, Missouri
STEPHEN F. LYNCH, Massachusetts
JIM COOPER, Tennessee
GERALD E. CONNOLLY, Virginia
JACKIE SPEIER, California
MATTHEW A. CARTWRIGHT, Pennsylvania
TAMMY DUCKWORTH, Illinois
ROBIN L. KELLY, Illinois
DANNY K. DAVIS, Illinois
PETER WELCH, Vermont
TONY CARDENAS, California
STEVEN A. HORSFORD, Nevada
MICHELLE LUJAN GRISHAM, New Mexico
Vacancy

LAWRENCE J. BRADY, *Staff Director*
JOHN D. CUADERES, *Deputy Staff Director*
STEPHEN CASTOR, *General Counsel*
LINDA A. GOOD, *Chief Clerk*
DAVID RAPALLO, *Minority Staff Director*

CONTENTS

HHS' OWN SECURITY CONCERNS ABOUT HEALTHCARE.GOV

Thursday, January 16, 2014,

HOUSE OF REPRESENTATIVES,
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM,
WASHINGTON, D.C.

The committee met, pursuant to call, at 9:36 a.m., in Room 2154, Rayburn House Office Building, Hon. Darrell E. Issa [chairman of the committee] presiding.

Present: Representatives Issa, Mica, Turner, Duncan, Jordan, Chaffetz, Walberg, Lankford, Amash, Gosar, Meehan, DesJarlais, Gowdy, Farenthold, Woodall, Massie, Meadows, Bentivolio, DeSantis, Cummings, Maloney, Tierney, Lynch, Connolly, Speier, Cartwright, Duckworth, Horsford, Lujan Grisham, and Kelly.

Staff Present: Ali Ahmad, Majority Senior Communications Advisor; Richard A. Beutel, Majority Senior Counsel; Brian Blase, Majority Professional Staff Member; Will L. Boyington, Majority Press Assistant; Joseph A. Brazauskas, Majority Counsel; Caitlin Carroll, Majority Deputy Press Secretary; Sharon Casey, Majority Senior Assistant Clerk; John Cuaderes, Majority Deputy Staff Director; Adam P. Fromm, Majority Director of Member Services and Committee Operations; Linda Good, Majority Chief Clerk; Meinan Goto, Majority Professional Staff Member; Ryan M. Hambleton, Majority Professional Staff Member; Frederick Hill, Majority Deputy Staff Director for Communications and Strategy; Michael R. Kiko, Majority Legislative Assistant; Matthew Tallmer, Majority Investigator; Sharon Vance, Majority Assistant Clerk; Rebecca Watkins, Majority Director of Communications; Tamara Alexander, Minority Counsel; Aryele Bradford, Minority Press Secretary; Susanne Sachsman Grooms, Minority Deputy Staff Director/Chief Counsel; Jennifer Hoffman, Minority Communications Director; Chris Knauer, Minority Senior Investigator; Elisa LaNier, Minority Director of Operations; Una Lee, Minority Counsel; Juan McCullum, Minority Clerk; Dave Rapallo, Minority Staff Director; Valerie Shen, Minority Counsel; Mark Stephenson, Minority Director of Legislation; and Cecelia Thomas, Minority Counsel.

Chairman ISSA. The committee will come to order.

The Oversight Committee exists to secure two fundamental: first, Americans have the right to know that the money Washington takes from them is well spent and, second, Americans deserve an efficient, effective Government that works for them. Our duty on the Government Reform Committee is to protect these rights. Our solemn responsibility is to hold Government accountable to taxpayers, because taxpayers have a right to know what they get from

their Government. We must work tirelessly in partnership with citizen watchdogs to provide the American people the facts and bring genuine reform to the Federal bureaucracy.

We are here today to ask and examine fundamental questions about the security of Healthcare.gov. We recognize best practices were not followed. Was securing testing completed before the launch to the satisfaction of the experts will be asked. What did top information security officials at the Center for Medicare Services and the Department of Health and Human Services recommend? Were the people who knew about the technology empowered? Were the decision-makers people who knew about the technology? Did leadership at CMS and HHS follow these recommendations? If there was disagreement between people below the top, were these questions and concerns properly delivered to higher-ups prior to the launch of the site?

By now the American people are well aware that there were functional problems in the Healthcare.gov website at launch. Many may know that other websites costing a fraction as much, but doing the same thing, worked better. For example, Kentucky and Hawaii launched sites that cost the Federal taxpayer about one-third as much and seemed to work better.

Those questions and others need to be asked, but today our real question is why does the Administration steadfastly deny the existence of security problems and shortcomings and lack of security testing, while in fact the experts, Federal employees, we hear from today will testify that there were known shortcomings and, in fact, unanswered questions at the time of the launch.

For many Americans, myself included, it seems to defy common sense that a website plagued with functional problems was in fact perfectly secure by design. Additionally, when an individual finds himself, while on one website, getting information delivered to him by mail acknowledging another individual from another State, we certainly know that there must be some cross-connect within the system that occurred, and that in fact was reported in the days shortly after the launch. This and other areas do concern this committee.

But most important, because we are the Oversight Committee for Federal contracting and Federal employees, our investigation has been active and attempted to get directly to the contractors, such as MITRE, who did an evaluation, that has been thwarted by the Administration, who warned and tried to interfere with this committee by asking vendors not to deliver us information. But through subpoena we have learned that in fact there were flaws that were reported. It is now undeniable that MITRE and other companies did their job sufficient for people to know an alarm was being sounded in the days before the launch.

We have acted to protect the information we received from those entities. Notwithstanding that, we have had repeated interference and claims that in fact we are the ones that are going to disclose a roadmap to hackers. What is so amazing is, in fact, the Administration would like you to believe that, first, there were no problems; second, any problems that there were, even though there were no problems, have been mitigated or, as I would quote or paraphrase the Administration, plans to mitigate are in place.

I have been in business a long time before I came to Congress. A plan to mitigate means you have not mitigated. Therefore, we will assume that any and all information given to us about known security risks at the time or prior to the time of the launch are still there.

Our witnesses today, for the most part, cannot refute that, because what we discover is they have not been personally assured, item by item, of the actual mitigation of those shortcomings. As I talk in circles to a certain extent, I do so because we continue to hear from the Administration there were no problems, the problems have been mitigated, and, oh, by the way, if you put out information about the problems others say exist, you are creating a roadmap to hackers.

I don't think anyone can square that; not my ranking member, not our witnesses. For that reason, again, this committee will continue to look at all reports of alleged security shortcomings or unknown areas, as in fact very, very important to keep private; and we will do so because we must assume that the website is still vulnerable, that the American people may, as we speak, be having their personal identifiable information hacked and taken, that in fact we cannot consider the website secure. If anyone would like to say the website is secure today, then I ask would you allow the former flaws to be put out there; and the answer, of course, will be no.

In Washington, people like to talk out of both sides of their mouth; they like to say there never was a problem, the problem there never was has been fixed, and, in fact, you may not put out records of the problems that never were because, in fact, they are known vulnerabilities. That is what we are facing today as we go into this.

It would be comical if it wasn't in fact all of your IRS records, links to Health and Human Services, of course, but links to the Department of Homeland Security and others. This website has tentacles into some of the most personal information, and in the future even more. More importantly, States have links into this same database; and, in fact, one of the things we know, which will not be the prime subject today, is that the States, for the most part, were not end-to-end tested, the States were not held to a standard of best practices. My only hope is that, as we look to the billions of dollars provided in Federal taxpayer money to the States, that in fact consistently they did a better job in both operational readiness and security. But that is but a hope. Today's hearing will be about the failures or at least the failures to use best practices that went into the launch of this site.

Lastly, in a few minutes I will be putting into the record a series of exchanges that went on between the White House and the Speaker, between the Secretary of Health and Human Services through her surrogates and the chairman; and I will do so because I think it is important to understand this is a serious, serious hearing. It is one in which the White House went to the Speaker of the House warning about the release of information and asking that information not be seen, not be heard, and not be delivered to this committee. It is one in which the secretary said she wanted to

meet, again, to me. I flew back and she refused to meet with me, even though she was in town.

I am deeply disappointed that we are here today still dealing with the inability to deal with what happened prior to October 1st, what has happened since October 1st, and I think most importantly a committee that on a bipartisan basis supports real reforms, real reforms that in many cases would have mitigated or eliminated some of the mistake made and would have allowed the President's signature legislation to not be marred by a website that failed to perform at its launch and is still questionable in its security.

Lastly, I certainly want to make sure that we all understand the American people know that companies have been hacked, that credit card information has been taken. It has been widely publicized. The difference between Target and other companies who dealt with hackers is we don't have to put our credit card into that machine at Target, we don't have to deliver that information; we have the choice of paying cash, we have the choice of not registering. We do not, no one on this dais has the ability to say I won't go into Obamacare; it is mandated by a law that I did not vote for, that the American people did not agree with, but went forward anyway on a purely partisan basis.

Mr. LYNCH. Mr. Chairman?

Chairman ISSA. So, therefore, I want to make it very clear we take serious that the standard for security on the Government side must be higher, and today's witnesses will help us begin the process of understanding how it could be higher.

I now recognize Mr. Cummings for his opening statement.

He is not recognized. The gentleman from Maryland is recognized.

Mr. LYNCH. Mr. Chairman, I just want to raise a point of order.

Chairman ISSA. The gentleman——

Mr. LYNCH. Are we going to balance out the time?

Chairman ISSA. The gentleman is not recognized. The gentleman is not in order.

Mr. LYNCH. I don't care to be recognized at all.

Chairman ISSA. The gentleman is not recognized.

Mr. LYNCH. You have gone on for 15 minutes. I am just asking for a point of order.

Chairman ISSA. The gentleman is not in order. Mr. Cummings is recognized.

Mr. CUMMINGS. Thank you very much, Mr. Chairman.

You are absolutely right, this is a very, very serious hearing. But I think we need to be very careful and be reminded that we have 110 million Americans, our constituents. You say they could use cash at Target. A lot of them don't have cash because they don't have jobs. Give me a break.

It is good to be here this morning. Today is the twenty-second hearing our committee has held on the Affordable Care Act. Twenty-two. We have spent more time on this one issue over the past three years than any other topic.

Mr. Chairman, I agree, we want to get this right. This is so very, very important. The consequences of what we do affect all of our constituents, and there are people watching us right now who are

suffering from dreadful diseases who are praying and hoping that we get it right. And I am determined to work hard with you to make sure that happens. But I am concerned about them, but I am also concerned about this 110 million of our constituents who have been placed in a vulnerable position with regard to their Target credit cards; and I am going to go further on that a little bit later.

So where are we today? The law that went into full effect, hello, full effect, on January 1st and now millions of people are getting health insurance they did not have before. They are receiving critical medical care; they have the security of knowing they will not be bankrupt if they get into an accident or get sick. But there is something more important or just as important as all of that: even under those circumstances, they are allowed to live in dignity. Dignity. That is what our Nation is all about, lifting up each other so that we all live in dignity. So this is a phenomenal accomplishment.

The law also put into place key protections for consumers, and I am so glad it did. I am so glad. Insurance companies are now prohibited from discriminating against people with cancer, our constituents, diabetes and other preexisting conditions, our constituents, both Republican and Democrat, both rural and urban. Insurance companies may not charge higher prices for women, and millions of people are now receiving free preventative care. That is so important. It is cheaper to keep somebody well than to treat them after they are sick. There are also huge financial benefits.

Health insurance companies are now sending rebate checks to millions of people. Since the law was passed, we have seen the lowest growth in healthcare costs in 50 years. If we repeal the law today, it would increase our deficit by more than $1.5 trillion.

Despite all of these positive results, Republicans are still obsessed with killing this law. After more than 40 votes in the House, they shut down the Government in an unsuccessful attempt to defund the law. Now they have shifted to a new tactic. This is brand new, hot off the press: scaring people away from the Healthcare.gov website.

Everyone agrees that initially the website's performance was seriously flawed. Our committee has a legitimate interest in investigating contractor performance and agency oversight, and we have held multiple hearings on this topic already.

But let me pause here for a moment. I am just reminded of what Emerson said, a favorite quote of Mandela. He said do not, do not be in fear and fail to act because of your fears and your problems, but be led by your hopes and your dreams. And this is about the hopes and the dreams of Americans to stay well, to make sure that their children are well, to make sure that if they get sick they don't have to go into bankruptcy. That is what this is all about.

And that is why you are right, Mr. Chairman, this hearing is serious, because it has consequences. In terms of security of the website, however, it is important to highlight all of the facts, instead of cherry-picking, I said it, cherry-picking partial information to promote a political narrative that is inaccurate. Based on the documents we have reviewed, and when I say we, I mean Republicans and Democrats, and the interviews we have conducted, I believe we can establish several key facts.

Number one, although some employees expressed concerns with security testing before this website was launched, the agency addressed these risks by implementing a strong mitigation plan as part of the Authority to Operate memo that was issued on September 27th.

Second, since that time the agency has complied successfully with the mitigation plan. The agency has now compelled full end-to-end security testing of the system and it addressed specific issues that arose in a timely manner.

Third, witnesses interviewed by the committee have praised the current level of security testing. They have described multiple layers of ongoing robust protections that meet, and in some cases exceed, Federal standards. As Ms. Fryer put it during her interview, the agency is using—and these are your words, Ms. Fryer; correct me if I am wrong—Ms. Fryer said, she is one of our witnesses, she said that the agency is using "best practices," Mr. Chairman, "above and beyond that which is usually recommended." So, Ms. Fryer, I hope you clear that up. Make it clear to us where you stand.

Finally, most importantly, to date there have been no successful attacks on Healthcare.gov by domestic hackers, foreign entities, or others who seek to harm our national security. Nobody's personal information has been maliciously hacked.

Now, we need to be careful. Obviously, this could change, given the increasing frequency and sophistication of attacks against all Federal IT systems. But the evidence obtained by our committee, and when I say our committee I mean Republicans and Democrats, indicates that the security of Healthcare.gov is strong and it keeps getting stronger.

In very sharp contrast, up to 110 million Americans were subjected to one of the most massive information technology breaches in history when their credit, debit, and other personal information was compromised at Target stores and online in November and December.

Mr. Chairman, I sent you a letter on Tuesday requesting a hearing on the Target breach, and I understand you have agreed to have our staffs meet on this issue next week, and I thank you for that. If our committee can hold dozens of hearings on the Affordable Care Act and on Healthcare.gov, which has not been successfully attacked to date, surely we can hold at least one hearing at the earliest possible date on the massive Target breach that affected more than 100 million of our constituents.

As I close, I want to close by thanking Dr. Charest. You have been pulling double duty, providing multiple classified briefings to Congress in addition to your day job. We thank you.

Ms. Fryer, your name has been thrown around on the House floor, when I am sure you have heard about it, but you have your opportunity today to clarify whatever it is you have to say.

And, Mr. Baitman, after finishing a day-long interview less than 36 hours ago, you were handed a letter inviting you to testify here today, and we thank you.

I want you all to know that we appreciate everything you and your staffs are doing to remain vigilant and constantly monitor the

security of the website. Millions of American families thank you for helping them.

With that, Mr. Chairman, I thank you and I yield back.

Chairman ISSA. I thank the gentleman.

I now ask unanimous consent that letters dated December 15th, 2013, from the White House; December 17th from this committee; an email exchange January 15th; and a letter to Secretary Sebelius on January 15th be placed in the record and copies be made and distributed. Without objection, so ordered.

Chairman ISSA. All members may have seven days in which to submit their opening statements and other information.

We now welcome our panel of witnesses.

Mr. Kevin Charest, Ph.D., is the Chief Information Security Officer at the Department of Health and Human Services; Ms. Teresa Fryer is the Chief Information Security Officer at the Centers for Medicare and Medicaid Services, which will undoubtedly be called CMS throughout the hearing; and Mr. Frank Baitman is the Deputy Assistant Secretary for Information Technology and Chief Information Officer at the Department of Health and Human Services, and, again, I thank you for back-to-back appearances.

Pursuant to the committee rules, would you please rise, raise your right hand to take the oath?

Do you solemnly swear or affirm the testimony you are about to give will be the truth, the whole truth, and nothing but the truth?

[Witnesses respond in the affirmative.]

Chairman ISSA. Please be seated.

Let the record reflect that all witnesses answered in the affirmative.

In order to deal with a fairly short period of time—one of our witnesses has a hard stop at 12, which we are going to very much try to respect, and we are likely to have a vote more or less at that time—I want to announce that I will ask you to stay within that five minute opening statement, and I will be very strict on the gavel today, which is not the history of this committee.

So we want everyone to ask their question and complete their questions well prior to five minutes. I won't cut off a witness answering a question, but I will cut off exactly at five minutes a question that is droning on, and I will curtail the answer of questions if, in fact, it is unable to be answered within a short period of time. And I say this because I want to get through all the people on the dais and allow our witnesses to leave timely.

Additionally, if witnesses need to excuse themselves for a short period of time, please just go ahead, signal to the clerk, do it, and use the facilities back here.

Other than that, Mr. Charest, you are recognized.

WITNESS STATEMENTS

STATEMENT OF KEVIN CHAREST, PH.D.

Mr. CHAREST. Good morning, Chairman Issa, Ranking Member Cummings, and members of this committee. My name is Kevin Charest and I am the Chief Information Security Officer for the United States Department of Health and Human Services.

The Department of Health and Human Services is the United States Government's principal agency for protecting the health of all Americans, providing essential human services, especially for those who are least able to help themselves. The HHS Office of the Secretary and the Department's 11 operating divisions administer more than 300 programs, covering a wide spectrum of activities.

The Office of the Chief Information Officer, in which I serve, is a part of OS. Our responsibility as one of the staff divisions of OS is to manage programs within OS and support the 11 operating divisions in carrying out their various and diverse missions. It is important to point out, however, that we manage the Department's information technology portfolio through a federated governance structure. The vast majority of the Department's IT resources are tied directly to the appropriations and statutory authorities Congress provides directly to our programs and operating divisions. Our governance authorities at the OS level reflect that federated structure. Thus, many of HHS's operating divisions have their own chief information officer, chief information security officer, and IT management structure. The exception of this rule is in OS, where the Department's CIO and CISO perform those responsibilities.

HHS's enterprise-wide information security and privacy program was launched in fiscal year 2003 to help protect HHS, including its operating divisions, against potential information technology threats and vulnerabilities. The program ensures compliance with Federal mandates and legislation, including the Federal Information Security Management Act. Under my leadership, I have established a framework for operating divisions to regularly report incidents involving IT security to my office. Operating divisions routinely report potential information security incidents to the HHS Computer Security Incident Response Center, which I oversee.

In addition to our internal investigation of all IT security incidents, we report all such incidents to the Department of Homeland Security's Computer Emergency Readiness Team at DHS's National Cybersecurity and Communications Integration Center. Through US–CERT's operations center, US–CERT accepts, triages, and collaboratively responds to incidents; provides technical assistance to information system operators; and disseminates timely notifications regarding current and potential security threats and vulnerabilities. For reference, in fiscal year 2013, US–CERT processed approximately 228,700 cyber incidents, an average of more than 620 per day, including Federal agencies, critical infrastructure, and industry partners.

It is important to note that HHS operates a defense-in-depth strategy for protecting its assets in accordance with guidance issued by the Office of Management and Budget and the National institute of Standards and Technology, which has been reflected in HHS's information security policy. This strategy includes the use of a risk-based approach to authorizing systems to operate, a robust set of technologies for continuous monitoring of systems, standards and minimum requirements for systems, as well as the appropriate business processes and controls to ensure the confidentiality, integrity, and availability of all HHS IT assets.

Consistent with these policies, CMS reports actual or suspected computer-security incidents in connection with Healthcare.gov to

the CSIRC. The reports are based on the operational security protections CMS has in place to deter and prevent unauthorized access, and weekly penetration testing and security scans of the system. CMS's chief information security officer and its information system security officer are responsible for designing and maintaining a security program to mitigate any risks identified in accordance with FISMA.

Additionally, building on Federal guidelines and regulations, and in conformance with industry standards, HHS has dedicated teams of career experts, including officials from the Office of the Chief Information Officer, the Office of Inspector General, Office of Civil Rights' Privacy Office, the CSIRC and key operating divisions who work around the clock to identify, manage, and mitigate suspected or potential breaches of PII.

In carrying out their work, those teams abide by HHS's PII Breach Response Team Policy, published in 2008, and HHS's Privacy Incident Response Team Charter, published in 2011. HHS security and privacy experts work with appropriate Federal Government and industry professionals to do the following: validate risk and review and approve response plans; review and approve communications or notice to affected individuals perform analysis on data in order to recommend strategies to effectively refine and improve the Department's response to the potential loss of PII; implement privacy and security solutions that can reduce the potential loss of PII; and, finally, monitor the privacy and security environment to raise awareness of threats to PII within the Department.

If the team determines that notification of a breach is warranted, the operating division coordinates through the PIRT to send letters to the affected consumers or businesses, informing them of the breach.

I appreciate the opportunity to meet with you today and discuss your interest in the Federal Government's IT security practices.

[Prepared statement of Mr. Charest follows:]

STATEMENT OF

KEVIN CHAREST

CHIEF INFORMATION SECURITY OFFICER,

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES

ON

HEALTHCARE.GOV

BEFORE THE

U. S. HOUSE COMMITTEE ON OVERSIGHT & GOVERNMENT REFORM

JANUARY 16, 2014

U. S. House Committee on Oversight and Government Reform

January 16, 2014

Good morning Chairman Issa, Ranking Member Cummings, and Members of this Committee. My name is Kevin Charest and I am the Chief Information Security Officer for the U.S. Department of Health and Human Services (HHS or Department).

The Department of Health and Human Services (HHS) is the United States Government's principal agency for protecting the health of all Americans and providing essential human services, especially for those who are least able to help themselves. The HHS Office of the Secretary (OS) and the Department's eleven Operating Divisions administer more than 300 programs, covering a wide spectrum of activities. HHS's Operating Divisions include: the Administration for Children and Families, the Administration for Community Living, the Agency for Healthcare Research and Quality, the Agency for Toxic Substances and Disease Registry, the Centers for Medicare & Medicaid Services (CMS), the Centers for Disease Control and Prevention, the Food and Drug Administration, the Health Resources and Services Administration, the Indian Health Service, the National Institutes of Health, and the Substance Abuse and Mental Health Services Administration.

The Office of the Chief Information Officer (OCIO), in which I serve, is a part of OS. Our responsibility, as one of the Staff Divisions of OS, is to manage programs within OS and support the eleven Operating Divisions in carrying out their various and diverse missions. It is important to point out, however, that we manage the Department's information technology (IT) portfolio

through a federated governance structure. The vast majority of the Department's IT resources are tied directly to the appropriations and statutory authorities Congress provides directly to our programs and Operating Divisions. Our governance authorities at the OS level reflect that federated structure. Thus, many of HHS's Operating Divisions have their own Chief Information Officers (CIOs), Chief Information Security Officers (CISOs), and IT management structure – the exception to this rule is in OS where the Department CIO and CISO perform those responsibilities.

My office convenes and leads the HHS Chief Information Security Officer Council, through which we and Operating Divisions' CISOs discuss and collaboratively develop Department-wide policies and share best practices and common tools involving IT security. However, program-level IT decisions, including those involving IT security, are made by our Operating Divisions at the Operating Division level, as in the instance of HealthCare.gov, the topic of today's hearing. As the "business owner" of HealthCare.gov, as is the case with Medicare.gov, CMS is responsible for IT security for the website. To date, there have been no successful security attacks on Healthcare.gov and no person or group has maliciously accessed personally-identifiable information (PII) from the site.

HHS' enterprise-wide information security and privacy program was launched in fiscal year 2003 to help protect HHS, including its Operating Divisions, against potential information technology (IT) threats and vulnerabilities. The Program ensures compliance with Federal mandates and legislation, including the Federal Information Security Management Act (FISMA). Under my leadership, I have established a framework for Operating Divisions to regularly report

incidents involving IT Security to my office. Operating Divisions routinely report potential information security incidents to the HHS Computer Security Incident Response Center (CSIRC), which I oversee.

Proactively identifying and addressing security "incidents" is a regular part of the process we require all Operating Divisions to employ. Security incidents include attacks and activities that may violate security policies, such as changes to system hardware without permission, the unauthorized use of hardware for accessing data, and attempts—either failed or successful—to gain unauthorized access to a system. A breach of PII may occur as a result of a security incident.

Often, upon further investigation, these security incidents turn out to be false positives. However, out of an abundance of caution, we investigate all such incidents to understand what actually occurred, and when necessary to develop an appropriate risk mitigation strategy to minimize future such incidents.

In addition to our internal investigation of all IT security incidents, we report all such incidents to the Department of Homeland Security's (DHS) Computer Emergency Readiness Team (US-CERT), at DHS' National Cybersecurity and Communications Integration Center. Through US-CERT's operations center, US-CERT accepts, triages, and collaboratively responds to incidents; provides technical assistance to information system operators; and disseminates timely notifications regarding current and potential security threats and vulnerabilities. For reference, in

fiscal year 2013, US-CERT processed approximately 228,700 cyber incidents, an average of more than 620 per day, involving Federal Agencies, critical infrastructure, and industry partners. It is important to note that HHS operates a defense–in-depth strategy for protecting its IT assets in accordance with guidance issued by the Office of Management and Budget and the National Institute of Standards and Technology, which has been reflected in HHS's information security policy. This strategy includes the use of a risk based approach to authorizing systems to operate, a robust set of technologies for continuous monitoring of systems, standards and minimum requirements for systems, as well as appropriate business processes and controls to ensure the confidentiality, integrity, and availability of all HHS IT assets in operation. In addition, HHS promptly notifies individuals of breaches that could compromise their protected information, when warranted.

Consistent with these policies, CMS reports actual or suspected computer-security incidents in connection with HealthCare.gov to the CSIRC. The reports are based on the operational security protections CMS has in place to deter and prevent unauthorized access, and weekly penetration testing and security scans of the system. CMS's Chief Information Security Officer (CISO) and its Information System Security Officer (ISSO) are responsible for designing and maintaining a security program to mitigate any risks identified, in accordance with FISMA.

In all cases, HHS takes mitigation of any IT security incidents, particularly those involving a PII breach, seriously and reviews Operating Division incident reports to ensure that mitigation solutions are applied appropriately and expediently. The process of determining risk and response begins immediately upon discovery of an incident:

- Employees are required to report any suspected or confirmed privacy incidents to each Agency's Incident Response Team or the HHS CSIRC as expeditiously as possible.
- The HHS CSIRC is required to report incidents involving PII within one hour to US-CERT.

Additionally, building on Federal guidelines and regulations, and in conformance with industry standards, HHS has dedicated teams of career experts, including officials from the Office of the Chief Information Officer, the Office of Inspector General, the Office for Civil Rights' Privacy Office, the CSIRC and key Operating Divisions, who work around the clock to identify, manage, and mitigate suspected or potential breaches of PII.

In carrying out their work, these teams abide by HHS's PII Breach Response Team Policy, published in 2008, and HHS's Privacy Incident Response (PIRT) Charter, published in 2011. HHS security and privacy experts work with appropriate Federal Government and industry professionals to:

- Validate risk and review and approve response plans;
- Review and approve communications or notice to affected individuals;
- Perform analysis on data in order to recommend strategies to effectively refine and improve the Department's response to the potential loss of PII;
- Implement privacy and security solutions that can reduce the potential loss of PII; and
- Monitor the privacy and security environment to raise awareness of threats to PII within the Department.

If the team determines that notification of a breach is warranted, the Operating Division coordinates through the PIRT to send letters to the affected consumers or businesses, informing them of the breach.

I appreciate the opportunity to meet with you today, and to discuss your interest in the Federal Government's IT security practices.

Chairman ISSA. Thank you.
Ms. Fryer?

STATEMENT OF TERESA FRYER

Ms. FRYER. Chairman Issa, Ranking Member Cummings, and members of the committee, thank you for the opportunity to speak about my role in protecting the security of the Federally-Facilitated Marketplace, also known as FFM. As a career civil servant, I have decades of experience in information security not only at CMS, but also at NASA, the U.S. Fish and Wildlife Service, Office of Personnel Management, and 20 years at security positions in the Navy. In my current role as Chief Information Security Office for CMS, my responsibilities include issuing CMS information security policy; ensuring the CMS systems comply with applicable laws and regulations; and providing oversight to maintain the confidentiality, integrity, and availability of all CMS information and information systems.

CMS has a long track record of successfully securing and protecting almost 200 complex IT systems related not only to FFM, but also to Medicare, Medicaid, and the Children's Health Insurance Program. In my role as CISO at CMS, I lead the team that is responsible for overseeing the independent security control assessments of CMS systems, including the FFM. These are conducted to assess the effectiveness of the security controls that CMS has implemented in the agency's information systems.

Independent security contractors completed a security control assessment of the FFM on December 18th, with no open high findings. This security control assessment met all industry standards, was an end-to-end test, and was conducted in a stable environment and allowed for testing to be completed in the allotted time. Given the positive results of the recent security controls assessment, the ability to complete comprehensive security testing and a mitigation plan in place, I would recommend the FFM to be given a new Authority to Operate when the current authority expires in March.

The FFM authorization to operate that is currently in place has s a number of strategies to ensure the FFM is protected against attacks and mitigates risk, including regular testing that exceeds best practices and a requirement to perform a full security controls assessment within 90 days of a launch. The risk mitigation strategies and compensating controls that were prescribed are being implemented and executed as planned. The protections that we have put in place have successfully prevented attacks. There have been no successful security attacks on the FFM and no person or group has maliciously accessed personally identifiable information.

As part of this mitigation plan, CMS established a dedicated security team, of which I am a member, to monitor, track, and ensure the activities in the ATO memo are completed. This team is responsible for the weekly testing, aborted devices, and Internet-facing web service and scans using continuous monitoring tools. Ongoing vulnerability assessments of the FFM network infrastructure and Internet-facing web service are conducted through penetration testing, which involves simulated attacks to breach the security defense of the website and continuous monitoring of marketplace-related systems to alert security professionals of any new

vulnerabilities that may exist due to recent changes or maintenance. Information from these tests has enabled us to prevent any successful attacks on the FFM.

While no serious security professional would ever guarantee that any system is hack-proof, I am confident, based on the recent security controls assessment and the additional security protections in place, that the FFM is secure. In many instances we have gone above and beyond what is required with layered protection, continuous monitoring, and additional penetration testing. CMS takes system security very seriously. My job is to anticipate and detect any possible security threat to our many systems, no matter how small. We continue to carry out this responsibility, protecting the FFM to ensure that consumers can use the system with confidence that their personal information is secure.

Thank you, and I am happy to take your questions.

Chairman ISSA. Thank you. Because we were not provided your opening statement, what date was that security assessment that causes you to recommend completed?

Ms. FRYER. It was completed on December 18th.

Chairman ISSA. December 18th.

Ms. FRYER. I am sorry. Yes, it was completed December 18th.

Chairman ISSA. Thank you.

Mr. Baitman.

STATEMENT OF FRANK BAITMAN

Mr. BAITMAN. Good morning, Chairman Issa, Ranking Member Cummings, and members of the committee. My name is Frank Baitman and I am the Deputy Assistant Secretary for Information Technology and the Chief Information Officer at the U.S. Department of Health and Human Services.

While I appreciate the committee's interest in Healthcare.gov, as you know, two days ago I spent eight hours in a transcribed interview with committee staff and with you and Representative Jordan, respectively, answering your questions. I received the committee's invitation to testify at today's hearing approximately 36 hours ago, at the close of Tuesday's transcribed interview. I will do my best to answer any questions you may still have, given the minimal time that I have had to prepare.

I would like to make clear to the committee the role of my office, that is, the Office of the Chief Information Officer for the Department of Health and Human Services in Healthcare.gov. I personally, and my office generally, have very little visibility into the development and operational oversight for the website. The Department manages its IT portfolio through a federated governance structure. Most of HHS's operating divisions have their own chief information officer and chief information security officer, one of whom is with us today, as well as their own IT management structure. The vast majority of the Department's IT resources are directly tied to appropriations made to our programs and operating divisions, and our governance structure reflects this reality.

Management and governance of Healthcare.gov was comparable to the management of similar IT initiatives throughout the Department's 11 operating divisions. And as with Medicare.gov and Medicare Part D prescription drug program, the development and secu-

rity of Healthcare.gov website has been led by CMS, which is the business owner for the system. Neither I nor my office had operational control over or responsibility for Healthcare.gov.

Since I jointed the Department less than two years ago, we have been working to restructure and update our IT governance to bring greater visibility into what the Department buys and builds across all of our 11 operating divisions. We are in the process of putting in place three It steering committees to bring together technology and program leaders from across the Department to improve our purchasing and management of information technology resources.

With respect to Healthcare.gov specifically, I would like to reiterate something that I have described to the committee on a number of occasions during my transcribed interview on Tuesday: Any discussions that I had regarding the rollout and launch of the website were based upon my past experiences in the private sector and the practices of tech companies that are often used. I did not have any personal, direct, or detailed knowledge of the development or security of the website, so it would not have been appropriate for me to make recommendations on operational decisions and, accordingly, I did not. As I also said in response to the committee's questions, it is totally appropriate and consistent with NIST guidelines that operational decisions about the technical aspects of Healthcare.gov be made by the administrator of CMS because of that individual's ability to broadly assess the acceptable risk for operating the system.

I am happy to answer any questions you may have, Chairman.

Chairman ISSA. Thank you.

Ms. Fryer, I am going to take you through a couple of quick slides here. They are all from the report that was not published. As they put up the side, these particular slides were provided to us after we initially interviewed you, and this was a memo never sent. Would you please tell us why this memo was never sent?

Ms. FRYER. So this was a memo that I initially was drafting to send to the chief information officer——

Chairman ISSA. Right. And you chose not to send it because of?

Ms. FRYER. Because events had taken place the next week with the chief information officer drafting the risk decision memo.

Chairman ISSA. In other words——

Ms. FRYER. So it was overcome by events.

Chairman ISSA.—events—okay. But it is still a good one for us to look at because it is consistent with your recommendations and your thought at the time.

So in slide 1 of the draft, you wrote, FFM does not reasonably meet the CMS security requirements which are intended to minimize CMS business risk. Is that correct?

Ms. FRYER. During the security assessment that was conducted in September, the security testing was not able to be completed; they weren't able to test completely——

Chairman ISSA. But these are your words.

Ms. FRYER. Yes.

Chairman ISSA. Okay. Additionally, you said there is also no confidence that personal identifiable information will be protected, correct?

Ms. FRYER. Again, there was security testing——

Chairman ISSA. But these are your words.

Ms. FRYER. I drafted this initial memo.

Chairman ISSA. Okay. And these are consistent with what you were saying in meetings in the September 20th time frame.

Ms. FRYER. This memo was capturing the briefing that we had given to Mr. Charest and Mr. Baitman and the CIO.

Chairman ISSA. Okay. So the other two witnesses knew that these are your words, but in a paraphrased what you told them. There is also no confidence that personal identifiable information will be protected. This is in slide 1A.

Ms. FRYER. Again, it was the results of the securing testing that had occurred.

Chairman ISSA. Okay. So in slide 1B you wrote, the independent assessor was forced to test different modules in multiple environments. In other words, no end-to-end, as it was going to be launched testing, correct?

Ms. FRYER. Yes.

Chairman ISSA. Okay. In slide 1C you wrote, complete end-to-end testing of FFM never occurred. That is correct, right?

Ms. FRYER. Yes.

Chairman ISSA. And that is best practices, of course, right?

Ms. FRYER. Yes.

Chairman ISSA. And you now testified in your opener that on December 18th end-to-end testing was completed and that is why you now have confidence that at least the snapshot of the site as it was that day would meet the requirements, subject to additional changes that occur in maintenance and modification, right?

Ms. FRYER. On the testing that was conducted on December 18th, yes.

Chairman ISSA. Okay. In slide 1C you wrote, the majority of the testing efforts were focused on testing the expected functionality of the application, not security, is that correct?

Ms. FRYER. Yes.

Chairman ISSA. Okay. Again, in slide 1C you wrote, several factors contributed to the limited effectiveness of the SSA modules and their interconnects. Can you expect that this could be a problem? And I guess in 1C you are saying yes, you are concerned about that area, is that right?

Ms. FRYER. Again, this was a memo that I was drafting; I didn't complete it, so some of these things hadn't been done.

Chairman ISSA. Okay. Slide 1C also says, valid test data was not provided prior to testing to give the true environment, correct?

Ms. FRYER. Yes. Normally, it is put into the system for the security testers beforehand, so it doesn't delay testing.

Chairman ISSA. So it is common to get real data, or at least data that is substantially real in both size and in cells and information in order to do a real assessment, and that wasn't done, is that correct?

Ms. FRYER. Test data was put into, yes, it was just a delay in getting the test data put into the system.

Chairman ISSA. Okay. So the two witnesses here were aware of essentially this information when you made your recommendation that it basically wasn't ready to launch, or at least you were un-

comfortable with whether or not it was ready because of the lack of end-to-end testing and the like, is that correct?

Ms. FRYER. My responsibility as the chief information security officer is to give an assessment to the chief information officer on the risks that were discovered during independent testing.

Chairman ISSA. And Mr. Charest, of course, was aware of this, plus had independent knowledge.

Mr. Baitman, yesterday in testimony you told us that you recommended a less than full rollout in a meeting, I believe September 10th, essentially saying with the problems and so on, best practices, in your opinion, would have been to roll out a portion of this rather than the size and scope that was rolled out on October 1st. You didn't characterize it completely as a recommendation, but it was certainly something you put out. In retrospect, would you prefer that to have been the way this site launched, in other words, more like a beta, in order to mitigate what we now know was pretty much a bad launch?

Mr. BAITMAN. Well, as you point out, Mr. Chairman, it wasn't actually a recommendation; it was a discussion topic for the meeting, and it was based upon my experience in the private sector, having seen this being done elsewhere. Sometimes it is referred to as a beta launch, a controlled, measured launch. In retrospect, I don't know that I can say because I didn't have direct knowledge of the system, the operational, development issues.

Chairman ISSA. Thank you.

Mr. Cummings.

Mr. CUMMINGS. Thank you very much, Mr. Chairman.

Over the past few months, House Republicans have made a number of extraordinarily unfounded claims about the security of Healthcare.gov. This scare tactic appears to be part of a coordinated campaign to frighten people away from Healthcare.gov's website. I want to make sure we separate fact from fiction today and tell the American people the whole truth.

I would like to go down the line with each of you and ask whether there have been any successful security attacks against the website.

Dr. Charest, let me start with you. You oversee HHS's Incident Response Team, is that right?

Mr. CHAREST. Yes, sir.

Mr. CUMMINGS. So if there is an attack on Healthcare.gov, you would know about it, is that right?

Mr. CHAREST. Yes, sir.

Mr. CUMMINGS. Dr. Charest, to date, I want you to look at me, now, has there been a single successful security attack against Healthcare.gov by a domestic hacker, foreign bad actor, or any other malicious individual group?

Mr. CHAREST. No, sir, there have been no reported attacks of any type of any malicious intent, either domestic or foreign.

Mr. CUMMINGS. Mr. Baitman, let me turn to you. You are the chief information officer at HHS. My constitutes and our constitutes are looking at you, they are depending on your information. Have there been any successful attacks against the website?

Mr. BAITMAN. There have been no reported successful attacks against the website.

Mr. CUMMINGS. Ms. Fryer, you are the chief information security officer for CMS. Have there been any successful attacks against the system?

Ms. FRYER. No, there have been no successful attacks.

Mr. CUMMINGS. So you all agree that over the past three and a half months, since the website has been live, there have been no successful attacks against the Healthcare.gov website, and I think that this is a very, very critical point.

Last November the CIO of Foreground Security testified before the House Energy and Commerce Committee, and this company is one of the contractors that conducts continuous security monitoring of the website. The CIO testified that nobody could guaranty with 100 percent certainty that Healthcare.gov was secure from external hackers. Do you all agree with that?

Mr. CHAREST. Yes, sir.

Ms. FRYER. Yes, sir.

Mr. BAITMAN. Yes, I do.

Mr. CUMMINGS. And he stated this, he said, "I also would say the same thing about Facebook or any banking website as well."

Dr. Charest, Mr. Baitman, during your interviews with the committee staff, you told us that you agree with this statement. You have both worked in the private sector. Can you both explain why Healthcare.gov is no more risky than commercial sites like Facebook? Mr. Charest.

Mr. CHAREST. Yes, sir. So, in essence, there are always vulnerabilities, there are a number of vulnerabilities. All of these sites rely on underlying infrastructure, third-party softwares. All of these variables coming together create an environment which can be compromised, candidly, at any time, so you have to be vigilant. As the defender, we have to defend against every possible attack and the attacker, in essence, has to find the one way in which we have not defended. So they are all always at some level of risk.

Mr. CUMMINGS. Now, Mr. Baitman, would you have anything to add to that or do you agree or disagree?

Mr. BAITMAN. I agree. No site is perfect, and we need to be vigilant, which is why we have layers of security.

Mr. CUMMINGS. Now, although there have been no successful attacks against Healthcare.gov to date, we have to keep in mind that there are constant attempts by malicious individuals and groups, both domestic and foreign, to attack large complex Government IT systems. We are all concerned about that, both Republicans and Democrats. We have to remain one step ahead of the actors.

I thank you for clearing all of this, the confusion that may have occurred. Our job is to ensure that the American people have accurate information so they are not wrongfully deterred from obtaining the critical healthcare coverage they need and deserve.

Now, I want to go to you just very briefly, Ms. Fryer. The chairman asked you some questions and I just want to summarize as I close. I want to make sure that I have this right, so let me ask you a series of very basic questions. The draft memorandum that he talked about, you are familiar, right?

Ms. FRYER. Yes.

Mr. CUMMINGS. Did you ever send the memorandum to anybody.

Ms. FRYER. No, I didn't.

Mr. CUMMINGS. Anybody?
Ms. FRYER. No, I did not, sir.
Mr. CUMMINGS. You never sent it to your boss, Mr. Trenkle?
Ms. FRYER. No, sir.
Mr. CUMMINGS. You never sent it to Administrator Tavenner?
Ms. FRYER. No, sir.
Mr. CUMMINGS. So you never pressed the Send button.
Ms. FRYER. No, sir.
Mr. CUMMINGS. During your interview with the committee staff, you explained that you stopped working on the memo and put it aside after you found out that your superiors were moving forward with the December 27th ATO, which included the mitigation measures we have been discussing, is that right?
Ms. FRYER. Yes, sir.
Mr. CUMMINGS. And did you ever finalize your draft memo?
Ms. FRYER. No, sir.
Mr. CUMMINGS. So you never finished it.
Ms. FRYER. No, sir.
Mr. CUMMINGS. Do you know if all of the information in the memorandum is accurate?
Ms. FRYER. No, sir. I was still validating the information.
Mr. CUMMINGS. Very well.
Thank you very much, Mr. Chairman.
Chairman ISSA. Thank you.
Mr. Mica.
Mr. MICA. Just a commentary. I heard the ranking member start out. I am as concerned. I came from a family that didn't have healthcare at times in our life, and there are 42 to 45 million Americans that don't have healthcare, and yet we have rolled out a flawed system. Everyone from the President of the United States to members of Congress on both sides of the aisle said the rollout, from a technical standpoint, was a meltdown and a fiasco. That was accessing it.
We signed up about a million people. I am one of the unwilling participants in that and others had no other choice, really, but we knocked six million people off of their healthcare system. This is a great record of success. And we probably left 41 to 44 million people still without healthcare. So I just had to comment when I heard that.
Ms. Fryer, you did in fact draft this memo of the 24th, right?
Ms. FRYER. Yes, sir.
Mr. MICA. That was up there. Yes. And it said that this platform basically doesn't reasonably meet the CMS security requirements which are intended to minimize CMS business risk, enterprise risk, or the application risk. There is also no confidence that the personal identifiable information will be protected. You wrote that on the 24th, right?
Ms. FRYER. Yes.
Mr. MICA. The 27th, what happened? Ms. Tavenner, didn't she sign the Authority to Operate? On the 27th she signed the Authority to Operate. Is that the event that overcame this? You wrote the memo. Who did you share the contents of this memo, that there wasn't assurance when this was rolled out? It is bad enough the thing wouldn't work from a technical standpoint or millions of peo-

ple who wanted healthcare couldn't access the system. In fact, I was served by a waitress the other day and she says, I wanted to get on it; I still don't have it because I couldn't access it. But it was flawed from the standpoint of being able to access it or work from an operational standpoint, right? At least initially, right?

Ms. FRYER. My responsibility was to brief my management and the chief information officer.

Mr. MICA. You are security, but you wrote that it wasn't ready for prime time rollout for security, right? And then you said events that overtook this. Well, the event was, in fact, that Tavenner, she signed the ATO. Did you sign the ATO?

Ms. FRYER. No, I did not. It is not my responsibility.

Mr. MICA. In fact, I saw at the end of the ATO you put a little caveat to protect your rear end, kind of, you put this paragraph at the end of the ATO, didn't you?

Ms. SPEIER. Mr. Chairman?

Ms. FRYER. My responsibility is to brief the CIO on its face.

Chairman ISSA. The lady will suspend. The gentleman will suspend.

Ms. SPEIER. Mr. Chairman, I would like to suggest that we all——

Chairman ISSA. No, the gentlelady will state her point of parliamentary inquiry, please.

Ms. SPEIER. Personal privilege.

Chairman ISSA. Point of personal privilege. Please state it.

Ms. SPEIER. Mr. Chairman, I think that we should show respect to the persons who are——

Chairman ISSA. That is not a point of personal privilege. Please state a point of personal privilege.

Ms. SPEIER. Well, I am offended by the fact that——

Chairman ISSA. Okay, if the gentlelady can organize an actual procedural request, we will reconsider it at that time.

The gentleman may continue.

Mr. MICA. Well, I understand, and, again, protecting yourself, I may have used a term that some member found offensive, but protecting your rear end, everybody knows it around here.

Ms. Fryer, last December you testified to the committee that prior to the October 1st launch you recommended again to deny the exchange's Authority to Operate, also known as the ATO, which is a document necessary to the website for the record. Is that accurate?

Ms. FRYER. Yes.

Mr. MICA. Why did you make this recommendation?

Ms. FRYER. The testing in September, there were some issues that were encountered during the testing, so there was a level of uncertainty as to the known risk.

Mr. MICA. Who did you make the recommendation to?

Ms. FRYER. My responsibility is to make the recommendation to my management and the chief information officer of CMS.

Mr. MICA. Okay. Ms. Fryer, you also testified that you communicated your recommendation to Mr. Trenkle and he shared your concerns, is that correct?

Ms. FRYER. Yes.

Mr. MICA. Did he sign the Authority to Operate, again, the ATO?

Ms. FRYER. No, he did not.

Mr. MICA. He did not. When did you learn Mr. Trenkle was also not comfortable enough to sign the ATO?

Ms. FRYER. It was probably during our conversation, during the security testing, when there were problems that were being encountered.

Mr. MICA. So that was earlier.

Ms. FRYER. And on September 20th, when I briefed him, Mr. Trenkle, and Mr. Baitman and——

Mr. MICA. Did Mr. Trenkle tell you why he decided not to sign the ATO?

Ms. FRYER. No, he did not.

Mr. MICA. Did you ever brief Administrator Tavenner on the security risks in the federal exchange?

Ms. FRYER. No, I did not.

Mr. MICA. Did you——

Chairman ISSA. The gentleman's time has expired.

Mr. MICA.—Mr. Charest and also Mr. Baitman?

Chairman ISSA. You may answer.

Mr. CHAREST. No, sir, I never briefed Tavenner.

Mr. MICA. Mr. Baitman?

Mr. BAITMAN. I am sorry, could you repeat the question?

Mr. MICA. Did you counsel with Ms. Tavenner on security issues?

Mr. BAITMAN. No, I did not.

Mr. MICA. Thank you.

Chairman ISSA. Thank you very much.

The gentleman from Massachusetts, Mr. Tierney, is recognized.

Mr. TIERNEY. Thank you very much.

Thank all the witnesses for their work and for being here again today.

So essentially what we have established is that we have a memorandum that allows the majority apparently to raise the spectre of problems, only to find out that it was never sent to anyone because those issues had been addressed and dealt with, and now we have a system that has not had any successful hack attack since then. But we continue to go over and over and over this because, if we do go over and over and over it, maybe somebody will think that there is a real problem.

But let's talk about the real problem. So we have spent a lot of time doing that on this committee, Oversight Committee, had hearings and subpoenaed documents, conducted interviews; Mr. Baitman ad nauseam with respect to you, at least. The good news is that there have been no successful attacks in security against the website, but every day people do attempt, from time to time.

So I have a modest suggestion here. Why don't we try to find out who is doing that? This is an oversight and investigatory committee, after all. It seems to me that if we have a website and people want to have healthcare, but there are people trying to prevent them from doing that, by that I don't reference my colleagues here, I reference people that are trying to—although many people are tiresome of the efforts to repeal—I am talking about people that are trying to get into the system and destroy it. We ought to go after those bad guys on that basis.

There are reports out there, pretty wide range set of reports, describing some of the malicious groups that are organizing to try to do this. One example is a group that developed a program called Destroy Obamacare. Are you familiar with that, Mr. Baitman?

Mr. BAITMAN. Yes, I have seen reports of it.

Mr. TIERNEY. And apparently what they were doing was trying to have a denial of service tool. Can one of you explain what that is? Mr. Charest?

Mr. CHAREST. Yes, sir. So in the case of Destroy Obamacare and in all denial of service tools, the basic premise is to flood the website with potentially even appropriate traffic, but such that legitimate users cannot access the site, it is overloaded, in essence.

Mr. TIERNEY. So the spectre this would raise is trying to be made true by people who are taking an overt action, trying to interfere with the system, would that be right?

Mr. CHAREST. Yes, sir.

Mr. TIERNEY. So press reports indicate that these are, in their words, right-wing groups motivated not by financial gain, but sort of a political animus. They disagree with the Affordable Care Act, so they are trying to intentionally block applicants from actually getting access and getting the rights entitled to them under the law. Is it a crime, Dr. Charest, for them to do this?

Mr. CHAREST. I am not an attorney, sir, but I believe it is.

Mr. TIERNEY. And who investigates those types of attacks?

Mr. CHAREST. In the event—and we did investigate the Destroy Obamacare code and those—not the actors, that is not our role, but the attempted attack. We found it to be rudimentary, but we did report, as we report all these incidents, to the Office of the Inspector General, and they received that information and would indeed investigate, if appropriate.

Mr. TIERNEY. Okay. And would they investigate to try to determine who the individuals leading this attack are?

Mr. CHAREST. That is my understanding, sir, but they would have to tell you their procedures.

Mr. TIERNEY. Okay. And perhaps that is a good action for this committee, would be to meet with those people and find out where they are going and what they are finding out. Does your incident response team, in terms of checking out these allegations to look to see who is undermining it, do you look to see how you can trace back on the site, where it may originate or where the site is hosted?

Mr. CHAREST. Yes, sir. We will trace back what we call the command and control, all the elements of the attack, as best as we can, and then we will share that with DHS, law enforcement, and others, as appropriate.

Mr. TIERNEY. And do you think that if the right people were investigating this, they would be able to in fact locate and find who these people are? Is there a likelihood of that?

Mr. CHAREST. It is possible, sir, but these things are fairly mercurial. IP addresses are rapidly changing; websites come up and down pretty often. The reality is, though, very often they are found.

Mr. TIERNEY. And it is because of that mercurial aspect and other things in constant attacks that you have the need for layered security, is that correct?

Mr. CHAREST. Yes, sir.

Mr. TIERNEY. And that layered security, once again, has been successful to date in stopping any successful hacking attack, is that correct?

Mr. CHAREST. Yes, sir, to date it has.

Mr. TIERNEY. All right. But because all systems, whether they are private or public like this, are constantly under attack, we have to be vigilant, and that is exactly what all of you are doing, is that correct?

Mr. CHAREST. Yes, sir, around the clock.

Mr. TIERNEY. Well, I thank you for your efforts.

Mr. Chairman, I think that I would ask that the committee consider an investigation pursuing those who are making attempts to attack and hack this site, for whether it is political animus or any other means on that. I think that would be an appropriate activity for us to do. That seems to be the real danger here, interfering with people's rights to have healthcare under the plan.

Chairman ISSA. The gentleman absolutely is right. Cybersecurity is part of our core jurisdiction. Mr. Connolly and I also spoke this morning at a cloud computing conference, so that is an area of not only interest, but a willingness to put staff and dais time into.

If I may, Mr. Cummings and I have been discussing, and I will be brief, the fact that we need to link in, as part of our committee jurisdiction, other areas of best practice flaws within the Federal Government, but also a recognition that those things have to be rippled out to private corporations; the banking community. Certainly Target has been mentioned here, but it wasn't the only commercial site hacked during this period of time. So I join with the gentleman and you can count on there being a series of briefings and possible committee hearings on them.

Mr. TIERNEY. I thank the chairman. Yield back.

Chairman ISSA. We now go to the gentleman from Michigan, Mr. Walberg.

Mr. WALBERG. Thank you, Mr. Chairman, and thanks to the witnesses for being here.

Ms. Fryer, we have dealt with the memo and your ultimate decision not to send it, but I think there is still questions that are there and it can't be just simply an out of sight, out of mind issue, so let me ask you a question. In your testimony last month before the committee you characterized the mitigation plan identified in the risk decision memo as "added protections to compensate for those unknown risks." What did you mean by this, specifically those unknown risks?

Ms. FRYER. So the security testing in September was not to the level that was expected, so they weren't able to test fully for the confidentiality and integrity areas. So in order to compensate for those compensating controls, we added those. Those were additional protections for the overall marketplace system.

Mr. WALBERG. Well, is a mitigation able to effectively address the vulnerabilities in the nearly half of the modules that made up the marketplace that were not fully security tested?

Ms. FRYER. It was a later protection, so later protection was put into place to mitigate the risk of those. You can't mitigate unknown risks, so, again, we have those later protections in place.

Mr. WALBERG. Well, based upon that, let me go, Ms. Fryer and Mr. Charest. Is it true that a good security control assessment makes it easier to create a good, tight mitigation plan?

Mr. CHAREST. I would say so, yes, sir.

Mr. WALBERG. Would you agree, Ms. Fryer?

Ms. FRYER. Yes, I do, sir.

Mr. WALBERG. Is it true that the more understood the risks, the better it is to create a plan to address those risks? Mr. Charest, Ms. Fryer?

Mr. CHAREST. Yes, sir, it is.

Mr. WALBERG. Just establishing the pattern here.

Ms. FRYER. Yes, sir.

Mr. WALBERG. Is it possible to mitigate unknown risks?

Mr. CHAREST. I don't know of any way to do that, sir.

Ms. FRYER. No, sir.

Mr. WALBERG. How difficult is it to mitigate unknown risks?

Mr. CHAREST. There are always unknown risks, so when you say how to mitigate a specific unknown risk, obviously, it is unknown, so what you do is you create an environment as we have, which is a defense in depth strategy; it is the infrastructural components, it is the methodologies that you utilize for your IT systems. It is the preponderance of all of these elements and then those teams that are designed to watch those elements in operation that will allow you to, in essence, address unknown risks.

Mr. WALBERG. But clearly with this testimony, to advance the rollout with unknown risks out there, with unclear mitigation, certainly appears, I think, to this committee to be a concern worth addressing and worth having these hearings over.

Chairman ISSA. Would the gentleman yield?

Mr. WALBERG. Yes, I would.

Chairman ISSA. I think the gentleman makes an extremely good point, and I might note that Ms. Fryer had made it clear that there were tests that could have been done that would have caused the unknown risks to be less unknown.

Mr. WALBERG. I concur.

Mr. Baitman, Teresa Fryer had a discussion with you about the security risk of Healthcare.gov, is that correct?

Mr. BAITMAN. There was a video conference call, I think you are probably referring to, on September 20th.

Mr. WALBERG. But you had a discussion with Ms. Fryer.

Mr. BAITMAN. She participated, that is correct.

Mr. WALBERG. What did Ms. Fryer tell you in that video conference call?

Mr. BAITMAN. As I recall, the CIO of CMS at the time was Tony Trenkle, and I believe Tony said that both he and Ms. Fryer were uncomfortable with signing the ATO.

Mr. WALBERG. Did you relay that discomfort with anyone about Healthcare.gov who had the Authority to Operate within HHS?

Mr. BAITMAN. I am sorry, I don't understand.

Mr. WALBERG. Did you relay Ms. Fryer's discomfort with the risk in signing the Authority to Operate with HHS?

Mr. BAITMAN. Yes, I did.

Mr. WALBERG. Did you tell this information to anyone, including Ned Holland or Jim Corr?

Mr. BAITMAN. I shared it with a few people, Ned Holland and Deputy Secretary Corr, yes.

Mr. WALBERG. What did you tell them?

Mr. BAITMAN. I thought it was noteworthy that the chief information security officer for CMS had expressed that she was uncomfortable signing it. On the other hand, I didn't consider it a red flag. So I wanted to share it with them, but Ms. Fryer wasn't the operational security person and CMS has an official who is responsible for that, so I thought that he was probably in a better position to know what changes had been made and what was going to launch on October 1st.

Chairman ISSA. The gentleman's time has expired.

We now go to the gentleman from Massachusetts, Mr. Lynch, for five minutes.

Mr. LYNCH. Thank you, Mr. Chairman, and I thank the ranking member as well.

Mr. Baitman, I want to go back some previous questioning. I am not sure if it was Mr. Cummings or Mr. Tierney, they talked about the beta approach that you referred to, and I just want to be clear on this. During your interview with the committee you had said earlier that your suggestion about the beta approach was based on your sort of general experience in the private sector with the rollout of IT systems, again, in the private sector, is that correct?

Mr. BAITMAN. That is correct.

Mr. LYNCH. Okay. So you explained your suggestion had nothing to do with security concerns with regard to the website.

Mr. BAITMAN. No. I didn't have any direct knowledge of functional or security issues; it was more of a this is a big, large, complex system and this is an approach that will minimize any challenges.

Mr. LYNCH. Okay. I just wanted to be clear on it. And, in fact, you told us in your previous testimony on September 10th that you had no specific knowledge of any security concerns with the website. Is that still correct?

Mr. BAITMAN. No specific concerns, no.

Mr. LYNCH. Okay. All right. Thank you.

I know we are talking about the technology, and in a moment of complete disclosure, I voted against the Affordable Care Act for a whole slew of reasons. However, this was not one of them. This was supposed to be the easy part, this rollout, the mechanical function of getting everybody up and on the system, so it is particularly discouraging. But I do want to say this is the law. I voted against it because I didn't think it was being done the right way, and people can differ on that. But I see my role going forward as one of making sure that the people that I represent have decent affordable, high-quality healthcare. That is my role going forward, and I think that should be everyone's goal here. But I have had an opportunity to sit with the folks that are running the Massachusetts Connector, the Health Connector, and some of the folks that are going out to sign everybody up, and I had one question.

I read the security documents for the Massachusetts Health Connector. Of course, I can't locate it right now, but what they do say in the security section regarding personally identifiable information, it talks about all the precautions they are taking, but then it

says, and it is sort of an odd wrinkle, however, once you voluntarily submit personally identifiable information to us, the Health Connector, related to your use of the portal, its dissemination is governed by the public records law, the Fair Information Practices Act of Massachusetts General Laws 66(a), so forth, and other applicable laws and regulations. And they have this one called out in bold, it says, for this reason, part or all of the information you send us may be provided to a member of the public in response to a public records request.

Now, I don't think that is what we intended when we passed that law in Massachusetts, but I know there are a whole lot of laws all across probably in all 50 States and the District of Columbia that have this public records access ability. And I am not sure if Mr. Charest or Ms. Fryer or you, Mr. Baitman, might have some comment on that. Is that something that we are going to have to go back, all 50 States, and say we don't mean that your personal information should be accessible through a public records request? Have you thought about that?

Mr. BAITMAN. I have to say I don't think I am in a position to address that, unfortunately.

Mr. LYNCH. How about you, Ms. Fryer?

Ms. FRYER. Same here, sir.

Mr. LYNCH. Okay. Mr. Charest?

Mr. CHAREST. I am from Massachusetts and, unfortunately, I still can't address it, sir.

Mr. LYNCH. That's three strikes and I am out, I guess. Well, I just want to say I appreciate your efforts and your good work on this, and I will yield back the balance of my time.

Chairman ISSA. Would the gentleman yield?

Mr. LYNCH. Sure I will. Sure I will.

Chairman ISSA. Mr. Baitman, I just had one quick follow-up, I think Mr. Lynch would also want to know. You said that Ms. Fryer's concerns did not raise a red flag. Do you really mean that her being uncomfortable with the security launch didn't raise a red flag simply because, even though she was knowledgeable, she wasn't "the one in charge"?

Mr. BAITMAN. That is what I mean, yes.

Chairman ISSA. I wish you had said that yesterday in the testimony.

Mr. Meehan is recognized for five minutes.

Mr. MEEHAN. I thank you, Mr. Chairman.

Mr. Charest, what is a successful attack on the system?

Mr. CHAREST. It can be defined, I suppose, in a number of ways, sir, but basically where the attacker actually has penetrated the system and/or compromised the system or, as we call it, exfiltrated, meaning taken away something from the system.

Mr. MEEHAN. Okay, so at this point in time, then, and this is the testimony. I am kind of interested in, on the record—and the chairman or the ranking member went through this with both you and Ms. Fryer and it has been your testimony there has been no reported successful attack on the system.

Mr. CHAREST. That is correct, sir.

Mr. MEEHAN. Now, I know from my work with chairing the Cybersecurity Committee for Homeland, a million hits a day on our

banking systems and things like this, Chinese hackers now. The record indicates that Chinese hackers came in in November and tried to get into the system. The last time they have ever done it?

Mr. CHAREST. I just want to parse there are attempts all the time by would-be attackers.

Mr. MEEHAN. So that is what I am trying to say. So we have maybe 30, 40, 50,000 navigators around the United States dealing with personally identifying information; we have Chinese hackers doing millions of attacks a day; sophisticated Russians; we had sophisticated networks that broke into Target. They didn't know it, with the most secure systems, they didn't know it for quite a period of time, did they? But somehow there hasn't been a successful attack since this has rolled out, this system?

Mr. CHAREST. That is correct, sir.

Mr. MEEHAN. All right. I am still struggling with the idea of how this thing was approved, the ATO decision was made, from my work with FISMA. Now, let me ask you specifically. Was there a security assessment plan that was done prior to the ATO decision? Ms. Fryer, Mr. Charest? Ms. Fryer, was there a security assessment plan completed and done by HHS prior to the decision that was made?

Ms. FRYER. So let me clarify. There was a security test plan that was created before the testing was conducted in September, and, yes, there was a security controls assessment report that was completed after the testing was.

Mr. MEEHAN. Have you turned over that plan and that assessment to this committee?

Ms. FRYER. I can't answer that question.

Mr. MEEHAN. Will you turn over that plan and that assessment to this committee?

Ms. FRYER. I would have to bring that back to my agents.

Mr. MEEHAN. Why is that a difficult question? Will you turn that plan and that assessment over to my committee on Cybersecurity in Homeland Security?

Ms. FRYER. I believe that those documents have been turned over; they are sensitive documents. Usually, we don't like to have them out there, but I believe that——

Mr. MEEHAN. It is my understanding that, in fact, the testing preceded the completion of those documents, that plan and the final assessment. Is that accurate?

Ms. FRYER. The testing is conducted and then a security controls assessment report is delivered by the contractor.

Mr. MEEHAN. MITRE didn't have access to the full—doesn't it need access to the full scope of the network?

Ms. FRYER. I didn't understand that question, full scope. They have a scope——

Mr. MEEHAN. Did they have full access to the information system and the environment of the operation?

Ms. FRYER. They have access——

Mr. MEEHAN. Did they have, did MITRE, who was the contractor, is it your testimony that during the period of time when they were supposed to be preparing this report, which is required under the law, under FISMA, did MITRE have proper access to the information system and the environment of operation, specifically?

Ms. FRYER. The system that was being tested, yes.

Mr. MEEHAN. Well, was it the system that was being tested or the full system? Not the system that was being tested, because what we had was parts of the system being tested. But FISMA doesn't authorize parts of the system being tested, it requires, under the law, the entirety of the system.

Ms. FRYER. They tested what was in scope of the security test plan that was provided by FISMA.

Mr. MEEHAN. Well, that is why I want to see the security test plan; not for the parts of the security, but the entirety of the system. Was the security test plan dealing with the entirety of the system prior to the OTA being made?

Chairman ISSA. The gentleman's time has expired, but you may answer and I think include the words end-to-end, perhaps, if you think that is appropriate.

Ms. FRYER. If I understand, you are requesting the security test plan.

Mr. MEEHAN. I want the security test plan, I want the security assessment, and then I want the remediation that was by the contractor and HHS in which they resolved all of those issues and I want to know that they were all done prior to the approval of the OTA, which is required under the FISMA law.

Ms. FRYER. Yes, sir, and I will bring that request back.

Chairman ISSA. Thank you. I thank both of you.

I will note for the committee that we were unaware of the December 18th study; it has not been provided, even though we believe it would be appropriate pursuant to the subpoena that was already in place, and it is my intention to issue a new subpoena to make sure there is no doubt that that document that we were not aware of as of yesterday had not been provided.

And for the record, no, Mr. Meehan, those documents have not been provided by HHS.

Mr. Connolly.

Mr. CONNOLLY. Thank you, Mr. Chairman. It is my understanding, however, that an unredacted copy of the test results was subpoenaed and was provided to this committee.

Is that correct, Ms. Fryer?

Ms. FRYER. Yes, I believe the September testing documents. If it is the December ones, like I said, I have to bring that request back.

Mr. CONNOLLY. Okay.

Chairman ISSA. Mr. Connolly, if I may. I just want to make sure your question is clear. MITRE Corporation, pursuant to a subpoena, supplied us documents; neither Health and Human Services, nor CMS have provided any such documents. Thank you.

Mr. CONNOLLY. Thank you for the clarification.

And, Mr. Baitman, let me express my regret that you were given so little notice before being asked to testify here today, for a committee that insists on better compliance from various Federal agencies, and in a timely fashion. Sometimes we seem to have a double standard, or it might be perceived that way.

I want to ask about security, because I have to admit, when I heard some of the statements, especially the opening statement of the chairman, it sounded scary to me. It sounded like only Healthcare.gov represents a potential security, cybersecurity threat

that could compromise everybody's healthcare in America. And, of course, as you indicated, Mr. Charest, cybersecurity attacks are going on all the time, in the private sector as well as in the public sector. The game here is to stay ahead of it, to develop systems to try to prevent it, to track it down, and that is going to be an ongoing battle forever for everybody because of the nature of technology. Do you think that is a fair statement, Mr. Charest?

Mr. CHAREST. Yes, sir. We cybersecurity professionals believe we have excellent job security.

Mr. CONNOLLY. Okay. I want to ask about, because several of us wrote the chairman of this committee asking for clarification of protocols to safeguard sensitive documents, and, Ms. Fryer and Mr. Baitman, if I am hearing you correctly, there is reason to be concerned about providing us with very sensitive documents that could somehow be compromised, obviously unwittingly. Nobody on this committee would ever leak anything to the press. But leaving it around accidentally or whatever could in fact lead to the very result that presumably this hearing is all about trying to deter, which is the compromise of consumer information.

And I quote the president and CEO of MITRE, who wrote the chairman of this committee and said, "In the wrong hands, this information could cause irreparable harm to the basic security and architecture of Healthcare.gov and potentially the security of other CMS data networks that share attributes of this architecture." Is that a fair concern, Mr. Baitman, Ms. Fryer?

Mr. BAITMAN. I believe it is a fair concern. I think that those documents could, if they were made public, provide a roadmap to an attacker.

Mr. CONNOLLY. So the very thing we are having a hearing about today we could, again, unwittingly, actually be part of the problem if we don't establish clear guidelines, clear protocols for the securing of such information. Fair statement, Ms. Fryer?

Ms. FRYER. Yes. These are sensitive documents that are tightly controlled.

Mr. CONNOLLY. So were someone to leak them, for example, someone got them through, I don't know, a subpoena, for example, and somebody decided to, as the ranking member, the phrase he used, cherry-pick information and leaked it to the press, again, not that that would ever happen here, in this committee, but if that were to happen it could actually lead to the very compromise and degradation of the security systems you are trying to put in place, is that correct?

Ms. FRYER. Yes, it is.

Mr. CONNOLLY. Mr. Baitman, you want to comment on that? You come from the private sector. You are looking sort of at a little different air level on these issues, looking at how CMS and your own department are handling it. Are you comfortable that we have strict protocols in place here, on this committee, for example, such that your concern would be abated?

Mr. BAITMAN. I am not familiar with the protocols the committee has.

Mr. CONNOLLY. Ms. Fryer?

Ms. FRYER. Again, I am not familiar with the protocols.

Mr. CONNOLLY. You are not familiar with our protocols. So, Mr. Charest?

Mr. CHAREST. No, sir, I am not familiar with the protocols, but I am concerned.

Mr. CONNOLLY. Allegedly, we have asked an outside security agency to look at your security measures. Are you familiar with that? Do you know who the outside—because the Democrats, as far as I know, were not informed as to who that entity was and whether they have come to some kind of conclusion. Have you been made—you were here seven hours, Mr. Baitman. Anyone talk to you about that?

Mr. BAITMAN. I was unaware of that, actually.

Mr. CONNOLLY. So were we. I thank you. My time is up.

Mr. MICA. [Presiding.] The gentleman from Oklahoma, Mr. Lankford, is recognized.

Mr. LANKFORD. Thank you, Mr. Chairman.

Mr. Baitman, I want to follow up real quick on a statement that you had made earlier that the chairman had also mentioned about Ms. Fryer and Tony Trenkle had made statements or recommendations to say that they were not comfortable giving authority to operate based on security issues. You had said that was not a red flag to you because someone else has responsibility for that. Who is that other person who has responsibility?

Mr. BAITMAN. Well, as I understand it, the Healthcare.gov project was built across various parts of CMS, some of which were not under Mr. Trenkle's leadership. They also had a CMS official who was responsible for all operational security for Healthcare.gov, and that person was on the ground and obviously more closely focused on it. Ultimately, though, I thought it was appropriate that Ms. Tavenner, as the administrator for CMS, be the individual who accepted risk on behalf of CMS because the project was large and being done across various parts of CMS.

Mr. LANKFORD. As a leader that I have staff around me as well, I gather the information from multiple staff, then have to make the final decision. Do you know if Ms. Fryer's recommendations and Tony Trenkle's statements about the security is not ready and this is a high risk, was that given to Ms. Tavenner before she made her decision?

Mr. BAITMAN. I actually don't know.

Mr. LANKFORD. Would you assume that that would be given to her?

Mr. BAITMAN. I would assume she would be briefed, yes.

Mr. LANKFORD. Because it would be an issue to me to make a decision and then to find out later that I have staff around me that had recommended this was a bad issue, but that information never landed on my desk because someone stopped it.

So you passed on the information, Ms. Fryer that Tony Trenkle had given you to other folks, and it was their responsibility then to pass it on to Ms. Tavenner, or who was going to give that to her?

Mr. BAITMAN. Well, as I said, the project was run within CMS, so I assume that the various parts of CMS who were running the project were actually briefing Ms. Tavenner.

Mr. LANKFORD. Right. But you were the one on the phone with them, getting the information saying this security is not ready, we

are at a high risk. Does that stop with you or do you say, okay, someone—so that does not have a duty to be able to report or somebody else is going to pick that up?

Mr. BAITMAN. So during that conversation they actually told me that they were going to bring the decision for whether or not the ATO would be signed to Ms. Tavenner.

Mr. LANKFORD. Who is the they there?

Mr. BAITMAN. Tony Trenkle, who was the CIO at the time, and Teresa Fryer.

Mr. LANKFORD. Okay.

Ms. Fryer, were you part of that responsibility of reporting that to Ms. Tavenner?

Ms. FRYER. No, I was not.

Mr. LANKFORD. Do you know how that was reported to her or if it was?

Ms. FRYER. No, I don't know that.

Mr. LANKFORD. So you don't know if Tony Trenkle passed that on as well.

Ms. FRYER. No, I don't.

Mr. LANKFORD. In October of this last year Secretary Sebelius said, in an ideal world there would have been a lot more testing, but we didn't have the luxury of that, and the law said the go time was October the 1st. Before the committee, then, CMS Chief Operating Officer Michelle Schneider was also asked why October 1st was chosen as a launch date; she said, I'm assuming it was in the law or the regulation.

Ms. Fryer, is it your understanding that October the 1st was required by the law to be the launch date?

Ms. FRYER. No, I don't know that.

Mr. LANKFORD. Did anyone repeat back to you, no we have security issues and concerns, but we have to go October the 1st, that is the law?

Ms. FRYER. No, they did not.

Mr. LANKFORD. Mr. Charest, were you aware of any provision in the Affordable Care Act that required October the 1st as the launch date?

Mr. CHAREST. No, sir.

Mr. LANKFORD. Anyone say to you we have to keep moving because the law requires this?

Mr. CHAREST. No, sir. From my perspective, it was just a date in a project plan.

Mr. LANKFORD. How about you, Mr. Baitman, did you have any knowledge of the statute requiring October the 1st?

Mr. BAITMAN. I don't have any knowledge. When I joined HHS, it was already sort of ordained that October 1st was the date.

Mr. LANKFORD. Do you know of any particular reason to say we have security questions and issues, October the 1st, if that is not in statute, if we have issues, maybe we should stall this until we deal with some of the security issues and make sure we are ready to go?

Mr. BAITMAN. Again, we work on a federated structure, so CMS had direct knowledge of what the requirements were.

Mr. LANKFORD. Is there any possibility that there may be a mistaken belief about the October the 1st date, that the secretary

states obviously in October that the law requires this? Is it possible that the Administration was working on a misbelief that the law required October the 1st?

Mr. BAITMAN. I can't speak for why other people had their opinions of that.

Mr. LANKFORD. Mr. Baitman, you had testified you had suggested a phased rollout after some beta testing. Was that suggestion taken?

Mr. BAITMAN. It was a beta launch. No, that wasn't the approach that was taken.

Mr. LANKFORD. Did you ever ask anyone why? I mean, obviously, by mid-October, in quiet moments at your house, surely you had some thought it probably would have been better to do a phased launch of this thing. Do you have any idea why that suggestion was ignored or delayed?

Mr. BAITMAN. At the meeting that you are referring to, CMS indicated, and CMS was in the best position to know, that they were confident the system would be ready for October 1st launch.

Mr. LANKFORD. Confidence seems to be misplaced.

I yield back.

Mr. MICA. The gentlelady from Illinois, Ms. Duckworth, is recognized.

Ms. DUCKWORTH. Thank you, Mr. Chairman.

I strongly believe that when my constituents are dealing with the Government, the last thing they should be concerned about is that their personal data is being compromised. Information security should be a top priority for any Government website, so I would like the panel to sort of bear with me as we go through exactly what is in place, to make sure that I have a better understanding, because we have sort of talked about all different things.

Ms. Fryer, could you walk me through the security precautions? You mentioned that there were many different layers that are in place. Can you explain what those three layers of protection are, and what procedures and processes are used?

Ms. FRYER. Yes. So there is the operational security, the day-to-day activities; there is code software reviews, that is the operational marketplace security team that does those activities; and they also have continuous monitoring, they have a group that has continuous monitoring tools in place; and then there is my group that is the oversight for CMS, and we also have continuous monitoring tools in place, as well as penetration testers that try to go in and hack into systems and penetrate the systems. HHS also has tools insight into our systems. So there is a layered protection of security for all of our CMS systems.

Ms. DUCKWORTH. So basically you are saying that it is not just the team that reports to you, but there are other groups of Government employees and contractors who oversee and conduct day-to-day security activities, is that right?

Ms. FRYER. Yes. Yes, there are many business information system security owners that have the day-to-day security activities, as well as my office.

Ms. DUCKWORTH. Are there systems in place, for example, at CMS, to ensure that the code is security tested on an ongoing

basis, not just when it is first implemented, but on an ongoing basis with secure code reviews and software assurance?

Ms. FRYER. Yes. Any time a change is made to a system, they have to do code reviews, and there is a very strict change management process that is followed before the change is put into production.

Ms. DUCKWORTH. And then I also understand that there is a weekly, as you said on penetration protection, weekly scanning and penetration testing of perimeter devices such as firewalls, is that correct? Is that ongoing as well?

Ms. FRYER. Yes. So that is above and beyond best practices. We do weekly scans of all the perimeter devices and all the external web-facing servers that are related to marketplace.

Ms. DUCKWORTH. So touching on what you are saying about the best practices, are you confident that the security systems and procedures that are in place are well within or not superior to the best practices that are ongoing with similar types of security that is needed for other websites?

Ms. FRYER. Yes, I do.

Ms. DUCKWORTH. Mr. Baitman, how does that compare to industry?

Mr. BAITMAN. I would say that practices in the Federal Government generally exceed industry.

Ms. DUCKWORTH. Generally exceeds industry? Thank you.

Have all of these layers of security, Ms. Fryer, been in place since the website was launched in October?

Ms. FRYER. Yes, it has been.

Ms. DUCKWORTH. And they are still in place and ongoing?

Ms. FRYER. Yes.

Ms. DUCKWORTH. Does CMS have a security team dedicated to ensuring that these multiple layers of protection are overlapping and continue to be effective?

Ms. FRYER. Yes. That was part of the ATO memo. Myself, I am on part of that team.

Ms. DUCKWORTH. How often does that team meet, talk to one another, review the procedures?

Ms. FRYER. On a weekly basis.

Ms. DUCKWORTH. On a weekly basis. Thank you. Can you sort of talk about how these multiple layers help to protect confidential consumer information and how they interact? For example, I signed up for healthcare reform and, by the way, saved $60. I went from $295 a month for my healthcare plan to $239 a month for the exact same plan, so I am pretty happy I got a savings. But when I put all that information, how do I, as a customer, know that I am protected? I know this is a very broad question, but can you sort of sketch how those different layers work with each other, say with my personal information that I have entered?

Ms. FRYER. Well, there are different layers, again, so if there are attackers coming in from the inside, we have many protections to detect these attacks. As mentioned before, there has been no successful attacks, but attacks are being made all the time on the website, so we have these tools in place to detect anomalies, all these tools. Even if one tool doesn't pick it up, we have this layer of protection, so we have other various tools in place to detect.

Ms. DUCKWORTH. So you could, for example, if there is just an unanticipated pattern that emerges or certain things that are happening, you can actually identify, wait, something is going on here that is unusual, we need to take a closer look at it?

Ms. FRYER. Yes, we have tools that will pick up anomalies.

Mr. MICA. I thank the gentlelady.

Ms. DUCKWORTH. Thank you.

Mr. MICA. I thank the witness.

Mr. Meadows, the gentleman from North Carolina.

Mr. MEADOWS. Thank you, Mr. Chairman.

I want to follow up on Ms. Duckworth's questioning there, if I could, Mr. Charest. This question is to you. She went through a long list of all the security that has been implemented and you were very, it seemed like, caution in the way that you said that there was no malicious attacks. Has there been inadvertent personal information that has been shared with someone else in this particular website?

Mr. CHAREST. Yes, sir, there has.

Mr. MEADOWS. There has. How many times has that happened, personal information from someone else getting shared with an inappropriate person?

Mr. CHAREST. I don't know the exact count, but in the early stages of the launch there were a number, I think somewhere less than 10. But there were some that were reported both in the media and to us.

Mr. MEADOWS. All right, so somewhere less than 10. Now, it is interesting that you wouldn't know the exact number, because you are very emphatic that there had been zero malicious attacks, but inadvertent disclosure you can't give us an exact number.

Mr. CHAREST. Well, I, in fact, have the categories in front of me here, sir, if you would like me to give you the numbers.

Mr. MEADOWS. Just the number.

Mr. CHAREST. Okay, no problem.

Mr. MEADOWS. So how many total disclosures of personal information to other people have we had?

Mr. CHAREST. We classify these incidents by——

Mr. MEADOWS. Total numbers.

Mr. CHAREST. It would appear, from the numbers I have in front of me, there are 13 category one, which is where we put potential PII——

Mr. MEADOWS. Thirteen. Total numbers. Total numbers, 13.

Mr. CHAREST. That is what I have here, yes, sir.

Mr. MEADOWS. So there was no others. So it wasn't less than 10, it was more than 10.

Mr. CHAREST. Well, no, not necessarily, sir, because the 13 in the category don't always mean there was a disclosure. They also could be exposure, but not disclosure.

Mr. MEADOWS. Exposure, but not disclosure.

Mr. CHAREST. Yes, sir.

Mr. MEADOWS. Okay. Well, we will save that for another day, because I think what the American people want is honesty and transparency, and to hear you testify less than 10 and more than 13. But more problematic for me is for you to lead this group to say that there were no malicious intent, and yet knowing full well that

there has been disclosure. They just want honesty and transparency.

Wouldn't you agree, Ms. Fryer, that that is important?

Ms. FRYER. Yes, sir.

Mr. MEADOWS. Okay.

In that, you have testified before, so in your preparation today to come before, have you met with attorneys to prep you on your testimony?

Ms. FRYER. I have been briefed on what to expect.

Mr. MEADOWS. Okay. How long has that briefing taken place? How much time did you spend in that prep? How many days?

Ms. FRYER. It was over a few days, couple hours each day.

Mr. MEADOWS. Okay, so how many hours does it take to be briefed to tell the truth?

Ms. FRYER. It doesn't.

Mr. MEADOWS. Okay. So why would that have gone on? Have you ever been told, well, we would prefer that you don't answer a question that way by an attorney?

Ms. FRYER. No, sir.

Mr. MEADOWS. All right. Have you ever had your previous testimony looked at and said, well, we wish you hadn't have said that?

Ms. FRYER. No, sir.

Mr. MEADOWS. All right. So you believe that from an honesty standpoint that you can tell the American people that their private information will not be disclosed to a third party?

Ms. FRYER. As a result of the recent security controls testing, yes.

Mr. MEADOWS. Okay. So the recent security you are talking about in December, that security testing.

Ms. FRYER. Yes, sir.

Mr. MEADOWS. Now, we have been led by other testimony here that the website and programming and modules continues today. Is that correct?

Ms. FRYER. Yes, sir.

Mr. MEADOWS. So how do you, based on a security analysis done in December, assure that the modules that are being written as we speak are secure?

Ms. FRYER. Because, again, there is the operational security that the marketplace security team has in place every time they do either—and it is done during the security development life cycle of a system and any time change is made to code they have all types of different security testing that is done on a day-to-day basis.

Mr. MEADOWS. All right. But we will have additional security risks that have to be assessed.

Ms. FRYER. No, that does not mean to say there is additional security risk.

Mr. MEADOWS. Okay, when is the next independent security assessment going to take place?

Ms. FRYER. We are requiring one every quarter.

Mr. MEADOWS. Okay, so we can expect one and you will submit that to this committee?

Ms. FRYER. Yes, sir.

Mr. MEADOWS. Okay. And when will the next one happen?

Ms. FRYER. We are scheduling that right now for the books, which will happen in——

Mr. MICA. I thank the gentleman and the witness.

The gentlelady from California, distinguished gentlelady, Ms. Speier.

Ms. SPEIER. Mr. Chairman, thank you.

Let me just say at the outset how delighted I am that the committee recognizes the importance of protecting the security of personally identifiable information in data systems and, as such, is making it a focus, because I think that one of the next hearings we should have is one on the breach that took place at Target with 110 million Americans who were impacted, and Neiman Marcus that was impacted as well, and I understand there were a couple other retailers. So the potential for being hacked is real, it happens in Fortune 100 companies, and we should do our due diligence by making sure that efforts in the commercial sector are being as secure as possible.

Having said that, let's focus on the testing that took place, the most recent testing that took place. Ms. Fryer, when you were here on December 17th, that testing was ongoing at the time. My understanding is that it has been completed, is that correct?

Ms. FRYER. Yes, ma'am.

Ms. SPEIER. And since it has been completed, can you say with certainty that it was completed in a stable environment, that all security controls were successfully tested and that it was a full end-to-end security test?

Ms. FRYER. Yes, it was a full comprehensive end-to-end security test and it was completed in one stable environment.

Ms. SPEIER. All right. Having completed that, is it your understanding as well, Dr. Charest, that it was completed under those standards?

Mr. CHAREST. Yes, ma'am, Teresa related that to me.

Ms. SPEIER. So the purpose of this testing is to identify vulnerabilities in an IT system so that they can be remediated. Is that fair?

Ms. FRYER. Yes, ma'am.

Ms. SPEIER. Does the fact that the SEA testing identifies vulnerabilities mean the system is exceptionally risky?

Ms. FRYER. No. A security controls assessment is conducted to discover vulnerabilities so they can be mitigated.

Ms. SPEIER. So just like Target needs to do these assessments and determine if there are vulnerabilities, it is appropriate for you to do that within the ACA.

Ms. FRYER. Yes, ma'am.

Ms. SPEIER. Now, the December testing has been completed and you have seen the results of that testing. I have a question for all three of you.

Ms. Fryer, do you have any reason to believe that consumer information submitted in the system is not secure at this time, based on the testing?

Ms. FRYER. No, I did not.

Ms. SPEIER. Dr. Charest?

Mr. CHAREST. No, ma'am, I do not.

Ms. SPEIER. Mr. Baitman?

Mr. BAITMAN. No, I do not.

Ms. SPEIER. So this is like giving the system a clean bill of health, is that correct?

Ms. FRYER. Yes, ma'am.

Ms. SPEIER. Knowing full well that just like Target and Neiman Marcus and any number of other companies that have been hacked into, there are persons out there, around the world, attempting to hack into systems. But at this point in time, having done the testing, we can say with confidence that the system is not subject to being breached, is that right?

Ms. FRYER. Well, there always is a chance for vulnerabilities, but the testing was completed successfully, it had good results, so we are confident that the risks have been identified and they are being mitigated.

Ms. SPEIER. Now, CMS has been running the Medicare system for decades, and I guess my question is has there ever been a major data breach of that system?

Ms. FRYER. For the two years that I have been there, not that I know of.

Ms. SPEIER. And how about the IRS data system?

Ms. FRYER. I can't answer that.

Ms. SPEIER. All right.

I have one more question. This committee passed a bipartisan measure that is referred to as FITARA, which is the Federal Information Technology Acquisition Reform Act. It would give CIOs much more authority in terms of hiring personnel and being in control of their operation. Do you see that as appropriate and helpful in doing your job? Mr. Baitman?

Mr. BAITMAN. I think that we would be well advised to look at some of the challenges that we have not just with this project, but other software projects the Federal Government has done and identify solutions so that we do a better job of managing IT going forward.

Ms. SPEIER. So are you suggesting that we should amend FITARA and add to it? Are you familiar with FITARA?

Mr. BAITMAN. I am somewhat familiar with FITARA, but getting into specifics I am not prepared to do right now.

Ms. SPEIER. Maybe you could do us a favor and review FITARA and make any recommendations you think would be appropriate to augment that bipartisan measure.

I yield back.

Chairman ISSA. [Presiding.] Would the gentlelady yield?

Ms. SPEIER. I certainly will.

Chairman ISSA. I think the gentlelady's question is a good one, and perhaps the other witnesses could answer the question of do they think that budget authority and a single point of accountability would enhance these kinds of projects. Mr. Baitman commented on that yesterday, so perhaps asked that way your question could get a more illustrative answer.

Mr. BAITMAN. I certainly think that you get greater accountability when you have one person who is clearly in charge.

Chairman ISSA. Ms. Fryer?

Ms. FRYER. Again, I agree with Mr. Baitman that it would give greater authority if one person had budget authority, yes.

Mr. CHAREST. I also believe that to be true, and I believe it would increase efficiency, reduce cost, and have a number of other ancillary effects.

Chairman ISSA. Thank you.

Thank you, Ms. Speier.

Mr. Bentivolio.

Mr. BENTIVOLIO. Thank you very much, Mr. Chairman.

Ms. Fryer, Mr. Charest, Mr. Baitman, we are not here today to examine whether the Healthcare.gov website is safe to use. We have already established that the Healthcare.gov website was certainly not safe to use on October 1st and is likely not safe to use today either. While you claim the website meets, and even exceeds, security industry standards and claims that no breach of the website has occurred, contradictory evidence is in abundance and is overwhelming. This evidence includes well-documented examples of security problems, some systematic, of extreme carelessness.

For example, an email disclosure of vulnerability was identified that would allow an attacker to enumerate email accounts for individuals. In another example, a user logged into to the Healthcare.gov website and saw information from a completely different person's profile. For another example, security researchers discovered an open URL redirection bug, which allows users to visit the website thinking they were going to the legitimate Healthcare.gov website, but instead be redirected to a malicious website that would completely hack their computer. This was only fixed after it was discovered when the website was online.

Ms. Fryer, you recommended denying an ATO, a necessary Authority to Launch Healthcare.gov, correct?

Ms. FRYER. Yes, sir.

Mr. BENTIVOLIO. If officials had accepted your recommendation, would you have been prepared to suggest an alternative date or would it have been an indefinite delay?

Ms. FRYER. Again, that wasn't my responsibility.

Mr. BENTIVOLIO. Would you have recommended an alternative date or would it have been an indefinite delay, yes or no?

Ms. FRYER. Again, that is not my responsibility. I can't answer that.

Mr. BENTIVOLIO. What would you have done had your recommendation been accepted, if you had one? You are the IT person. Would you recommend a delay or an alternative day?

Ms. FRYER. My responsibility is not to determine whether or not to—when a system goes into operation, mine is, again, to identify the risks and make sure that they are being mitigated.

Mr. BENTIVOLIO. So you identify the risks, but you don't make any recommendations?

Ms. FRYER. I brief the chief information officer on the security risks, and there are many other risks that have to be taken into consideration when a system is going operational.

Chairman ISSA. Would the gentleman yield for a second?

Mr. BENTIVOLIO. Yes.

Chairman ISSA. I am not sure you were in the room, but 77 days after the launch Ms. Fryer did testify that she now has confidence that the end-to-end that she would have asked for and so on has been properly mitigated. So I think an answer to your question to

a certain extent is 77 days would have been enough because it occurred.

Mr. BENTIVOLIO. Thank you. Thank you.

Do you know whether Ms. Tavenner was informed of your concerns and your recommendations on the security risks?

Ms. FRYER. I am sorry, sir, I didn't hear the question.

Mr. BENTIVOLIO. Do you know whether Ms. Tavenner was informed of your concerns and your recommendations?

Ms. FRYER. I don't know that.

Mr. BENTIVOLIO. To your knowledge, what IT security expert did Ms. Tavenner rely on to override your concerns on the risks of——

Ms. FRYER. I can't answer that question.

Mr. BENTIVOLIO. Do you know if she spoke with any IT security experts prior to overruling your recommendations or——

Ms. FRYER. I don't.

Mr. BENTIVOLIO. You don't know.

Ms. FRYER. No, I don't know.

Mr. BENTIVOLIO. Thank you. That is all my questions.

Chairman ISSA. I thank the gentleman. We now go to the gentlelady from New Mexico, Ms. Grisham.

Ms. LUJAN GRISHAM. Thank you, Mr. Chairman, and I want to thank the panel for being here. It is clear that we are all concerned about securing the financial and health-related private information on the website. Whether it was this healthcare website or any other application by the Federal Government, that is going to be one of our priority concerns for our constituents, so I appreciate your attention and willingness to engage directly in this hearing.

And like everyone, I think, I am happy that there haven't been any significant or malicious security breaches to date, so that we are not seeing a significant problem with the security measures taken to date to protect that information for consumers and users. And, I want to make sure that that is the goal of this conversation, that we continue to do whatever oversight and enhance those security tests and measures all of the time, because every day those risks are greater because people figure out better and more enhanced ways to get access to that information; and given that I am from a State that has a particularly high uninsured population, we are going to have a high user end result, I hope, in the marketplaces and exchanges. So I want to go just back to a couple things.

Ms. Fryer, it is my understanding that the Federal Information Security Management Act defined the security control standards for all Government information technology security systems. Is the Healthcare.gov compliant with all the standards set forth in FISMA?

Ms. FRYER. Yes, security testing was conducted in accordance with FISMA.

Ms. LUJAN GRISHAM. And are CMS and HHS implementing additional controls or best practices beyond what is called for in FISMA?

Ms. FRYER. Yes, ma'am. We are exceeding industry best practices, as well as we have HIPAA controls in place.

Ms. LUJAN GRISHAM. And that is important to me because during our last hearing on Healthcare.gov it was clear that there were inherent security risks in any electronic system, so getting a sense

that you are going beyond that and looking at best practices is critical. Can you give me a sense of what exactly you are doing to continually monitor and mitigate security risks on the website, some examples?

Ms. FRYER. Again, we are keeping in place those additional above and beyond the additional requirements of the weekly scanning or continuous monitoring tools, the weekly scans of the external web-facing marketplace servers, and——

Ms. LUJAN GRISHAM. So you are going beyond the weekly scans. That is what I am trying to get at. Give me a concrete example of what in addition you are doing.

Ms. FRYER. Well, we are continuing those, those that are in the mitigation plan, so we are continuing that. And then there is the operational day-to-day security that is in place as well by the other group.

Ms. LUJAN GRISHAM. I appreciate that, and I would also encourage you to lead in best practices and do everything in your power to go back and describe that. It is certainly my opinion, and I would guess the opinion of many more, that you would do everything and enhance your mitigation plan to the highest degree and lead that for the Country, given the importance and the value of the information on the website. Thank you.

Ms. FRYER. Yes, ma'am.

Chairman ISSA. Thank you.

There was no question pending, was there? Okay.

I want to inform everyone that there is a vote on the floor. We are going to stay as long as we can. Mr. Baitman will not be here, if, and, or when we reconvene. You have a hard stop at 12 and we are clearly not going to be back in time for that. So we are going to go as quickly as we can.

Mr. Jordan.

Mr. JORDAN. Thank you, Mr. Chairman.

Ms. Fryer, the memo you wrote, but didn't send, dated September 24th, 2013, you testified earlier that the reason you didn't send it was because there were subsequent events that happened that caused you not to think that it was necessary to send, is that correct?

Ms. FRYER. Yes, sir.

Mr. JORDAN. Why didn't you send it, though, the day you wrote it? If things happened after the fact that tell you, oh, I don't need to send it, on September 24th, when you wrote this, you believed everything you wrote, correct?

Ms. FRYER. Yes. Yes. That was being prepared as a memo. Usually an ATO package would go up to the chief information officer, and that is a draft.

Mr. JORDAN. All I am asking is on September 24th, the date on the memo, when you wrote there is no confidence that personal identifiable information will be protected, that is a big pretty statement. Why didn't you send it that day?

Ms. FRYER. Because this was just trying to capture what was already briefed on September——

Mr. JORDAN. Something that important—again, you said it was events that happened the next week that caused me not to send it. But on that day you believed everything you wrote here. These

are big statements. Why not send it? Did someone talk to you and tell you, hey, Teresa, don't send that memo?

Ms. FRYER. No, sir. A decision had been made to elevate to Marilyn Tavenner.

Mr. JORDAN. That doesn't change the fact that you were going to send this to Mr. Trenkle, directly above you in the chain of command. I just wonder why you didn't send it. If I write all this stuff down, important stuff, and also based on testimony we had at a previous hearing, you were the only one who read the MITRE report prior to this memo. I would assume that had a big impact on why you wrote the things you did. All I am wondering is why you didn't send it. If I have this information, I know this thing is not ready, I do this memo, hard-hitting memo that says this thing isn't even close to being secure, no end-to-end testing is done, and then I don't send it.

Ms. FRYER. Because it was part of the ATO package that was not going up to Mr. Trenkle.

Mr. JORDAN. All right, let me change here a little bit. You were interviewed a month ago by the committee, and the young lady behind you, Ms. O'Connor, accompanied you in that interview, is that correct?

Ms. FRYER. Yes, sir.

Mr. JORDAN. And, Mr. Charest, you were interviewed last week and Ms. O'Connor also accompanied you in that interview?

Mr. CHAREST. Yes, sir, that is correct.

Mr. JORDAN. And, Mr. Baitman, you were interviewed two days ago and Ms. O'Connor also accompanied you to that interview, is that correct?

Mr. BAITMAN. That is correct.

Mr. JORDAN. In the interviews we learned, Mr. Charest, you said that there was a meeting on, I believe, September 10th, where all the key leadership folks from Ms. Tavenner, Mr. Corr, CMS and HHS were there, and after the meeting—you weren't at that meeting, Mr. Charest, but Mr. Baitman was. After that meeting, Mr. Baitman, you had a conversation, and here is the transcript. You said, after the meeting he recommended a delayed rollout. Your answer was, that's my recollection, yes. A delayed rollout of Healthcare.gov? Your answer, that's my recollection.

Now, two days ago, when we talked to Mr. Baitman, which I wasn't in your interview, but I was in Mr. Baitman's interview, Mr. Baitman said that was not accurate. Do you stand by the statement you made to the committee staff one week ago?

Mr. CHAREST. Yes, I do.

Mr. JORDAN. Okay, Mr. Baitman, he said that you said to him, in a conversation after that meeting, you recommended not rolling it out. Is that accurate?

Mr. BAITMAN. That is accurate. I am sorry, could you rephrase that? I am sorry.

Mr. JORDAN. You recommended not rolling out Healthcare.gov on October 1st.

Mr. BAITMAN. No, that is not.

Mr. JORDAN. So which one of you told the truth? Which one is lying and which one is telling the truth? Mr. Charest said you had

a conversation—now, you have worked with Mr. Charest for a while, Mr. Baitman?

Mr. BAITMAN. I have.

Mr. JORDAN. Do you have a good working relationship?

Mr. BAITMAN. We have a great working relationship.

Mr. JORDAN. Mr. Charest, is that accurate? You have worked with Mr. Baitman obviously a while. Do you have a good working relationship?

Mr. CHAREST. Yes, I do.

Mr. JORDAN. Do you normally understand, when he communicates to you, what he is saying?

Mr. CHAREST. Yes, I do, sir, but I——

Mr. JORDAN. So your recollection was he recommended, that Mr. Baitman recommended not rolling out Healthcare.gov. He is saying that is not what happened at all in that conversation.

Mr. CHAREST. With all due respect, sir, that is not exactly what I—my testimony, I was asked that question several times to sort of clarify what I meant by delayed rollout, and what I hope I made clear, and I would like to make clear here to you, sir, is that I didn't know exactly what he meant. This conversation took place, it was probably less than two minutes, literally, and it was four months ago, and I didn't ask him the details. To me, as an IT professional over 30 years, a delayed rollout could have been a phased rollout, which is actually what I was thinking it meant, but I didn't ask and he didn't offer. I don't know what he meant and that is my recollection, though.

Mr. JORDAN. But the point is there was no delayed rollout.

Mr. CHAREST. Not to my knowledge.

Mr. JORDAN. You understand that was what he wanted to do?

Mr. CHAREST. I understand that he made a recommendation——

Mr. JORDAN. You agreed with that, Ms. Fryer agreed with that, and it wasn't done.

Mr. CHAREST. No, it wasn't done.

Mr. JORDAN. Okay. Prior to coming today, did the three of you sit down with Ms. O'Connor and talk about what was going to take place at today's hearing, and discuss what kind of answers you might give, what kind of questions you might receive?

Mr. CHAREST. Yes, sir, I did.

Mr. JORDAN. Ms. Fryer?

Ms. FRYER. Yes.

Mr. JORDAN. Mr. Baitman?

Mr. BAITMAN. Yes, I did.

Mr. JORDAN. Oh, so you worked it out after you had this disagreement. One said that you said delay, then you said there wasn't. You sat down and talked this out?

Mr. BAITMAN. No, that isn't what happened.

Mr. JORDAN. Okay.

Mr. Chairman, I see I am over time. I yield back.

Chairman ISSA. I thank the gentleman.

We now go to the gentleman from Pennsylvania, Mr. Cartwright.

Mr. CARTWRIGHT. Thank you, Mr. Chairman.

I want to start off by giving Mr. Charest and Mr. Baitman a chance to more fully respond. My colleague just basically said one

of the two of you was not telling the truth, and I want to give you each a chance to fully talk about that.

Mr. BAITMAN. So let me begin. As I said earlier, at the September 10th meeting there was a discussion topic about a beta rollout. It was simply a discussion topic. I, after the meeting, mentioned it to Kevin Charest. That meeting was four months ago. I talk to Mr. Charest 10 times a day about various things in an operational capacity. This wasn't a high priority topic and I am sure that the words could have changed over time.

Mr. CARTWRIGHT. I thank you for that.

Mr. Charest?

Mr. CHAREST. Yes, sir. Basically, I don't believe that what I said is inconsistent with what I understand Mr. Baitman has been saying, which was an alternative rollout schedule. There are many different terms used in IT, and I may have just processed it that way, but fundamentally we are saying the same thing.

Mr. CARTWRIGHT. And my understanding is, just to be clear, Mr. Baitman's recommendation had nothing to do with security, is that correct, gentlemen?

Mr. BAITMAN. It simply had to do with my observation from seeing how other companies have rolled out large, complex systems to the public.

Mr. CARTWRIGHT. All right.

Now, Ms. Fryer, I didn't mean to leave you out. You are the chief information security officer at CMS. In that capacity you raised concerns in September about the status of security testing for the website, is that right?

Ms. FRYER. Yes, sir.

Mr. CARTWRIGHT. And during your interview with committee staff, you explained that in your roll as chief information security officer your job is to make recommendations to your boss, the chief information officer. At the time that was Tony Trenkle, right?

Ms. FRYER. Yes, sir.

Mr. CARTWRIGHT. You explained to the committee staff that your roll was not to make the final decision on whether to go forward, am I correct in that?

Ms. FRYER. Yes, that is correct.

Mr. CARTWRIGHT. The chief information officer, Mr. Trenkle, was a career executive with decades of experience, is that true?

Ms. FRYER. Yes, sir.

Mr. CARTWRIGHT. Did you have respect for Mr. Trenkle? Did you value his experience and his expertise?

Ms. FRYER. Yes, I did.

Mr. CARTWRIGHT. You told us during your interview that during the two years in your position Mr. Trenkle often accepted your recommendations, but there were other instances when he did not, and those were unrelated to the Healthcare.gov website. Am I correct in that?

Ms. FRYER. Yes, sir.

Mr. CARTWRIGHT. Now, in this case, Mr. Trenkle decided to recommend to Administrator Tavenner that she go forward with the Authority to Operate, but that was only after strong mitigation strategies were added to the ATO in order to mitigate against the risks you identified. Sitting here today, do you believe that you pro-

vided Mr. Trenkle with the information necessary to enable him to make an informed decision about moving forward?

Ms. FRYER. Yes. I provided him the risks that were discovered during testing from a security perspective. And as the chief information officer, he takes that in and there are many other teams that provide other risks, there are business risks, mission risks, and all that is taken into consideration when a decision is made to put a system into operation.

Mr. CARTWRIGHT. You said during your interview that Mr. Trenkle, in his capacity as chief information officer, had a broader perspective on various risks for the federally facilitated marketplace. So when he was making his evaluation, you were one of several sources from which he was receiving information, is that true?

Ms. FRYER. Yes, that is right.

Mr. CARTWRIGHT. Okay. Ultimately, Administrator Tavenner signed the Authority to Operate based on her recommendation from her chief information officer, Mr. Trenkle. So in your view of the appropriate rules and authorities of various CMS officials, do you believe Mr. Trenkle's actions complied with FISMA?

Ms. FRYER. Again, he was the one responsible for whether or not a system goes into operation. I can't answer or speculate as to what path he took, but, you know.

Mr. CARTWRIGHT. Well, thank you. My time is up and I thank all of you for coming today.

Chairman ISSA. Thank you.

Now we go to Mr. Woodall. Mr. Woodall, we are very close on time, so be as pithy as possible.

Mr. WOODALL. Thank you, Mr. Chairman, as we enter hour three. My questions are primarily for Ms. Fryer and Dr. Charest. I want to thank you both for your military service, as well as your service.

I understand you, Dr. Charest, have spent some time in the great State of Georgia over the years. We welcome you back. Any time you want to come back, bring your big brain and your pocketbook down there to spend with us.

Mr. CHAREST. Thank you, sir.

Mr. WOODALL. I want to talk about a meeting that took place back on September 23rd. I don't believe either of you all was there. It was a meeting with Michelle Schneider and George Linares and Tony Trenkle. You prepared a slide for that presentation identifying some of the high risks that you had found, Ms. Fryer, and I want to put a slide up on the wall. I want to ask you to help me understand this. This is about Authority to Connect agreements.

And what I want to look at is, from my reading of this slide, and I want you all to help me with it, it says 17 States did not have Authority to Connect agreements here on September 23rd, and the recommendation was to go ahead and allow these States to have day one operation authority notwithstanding the risks that are listed below; and those risks listed below include things like, in most cases, one or more reviews of security documentation have not been completed. In other words, no review of security documentation has been completed. And even more troubling, the third risk, CMS is accepting risk on behalf of its Federal partners, the IRS, DHS, and

SSA, which could have legal implications in the event of a data breach.

Am I reading this slide correctly, to say that in many cases no review of security had taken place, but it was the decision of CMS to assume the risk to allow these 17 States to connect on day one? Ms. Fryer?

Ms. FRYER. I can't speak to this slide; I did not have input into this slide. But I do know that CMS did establish a baseline of secure requirements that the States had to meet in order to be granted an Authority to Connect by the chief information officer.

Mr. WOODALL. There was such an authority in place, but what this slide says is in most cases not even one review had been completed, and we are willing to waive that responsibility and assume that risk for a period of 90 days. At least that is how I am reading this slide. But you are saying, as chief information security officer, you weren't involved in that decision-making at all?

Ms. FRYER. No. Again, this was the marketplace security team that was involved in the State-based security requirements.

Mr. WOODALL. Dr. Charest, is that something that you have seen before? There is not one colleague out of 434 that has the authority to accept risk on my behalf and on behalf of my constituents. This seems incredibly unusual, CMS is accepting risk on behalf of the IRS and the Department of Homeland Security. Is this something that you have seen before? We have talked about best practices a lot while we have been here. This seems alarming to me. Am I misreading what I am seeing on this slide?

Mr. CHAREST. Well, sir, what I can tell you is I have not seen this other than it was shown to me during my transcribed interview, but basically this is a PowerPoint presentation, so when I look at that, I am assuming, and I would have to assume it, that some discussion between CMS and those entities it is indicating it is accepting risk for took place.

Mr. WOODALL. Again, we have talked a lot about best practices today. Is it best practices to, again, while formal testing has not been completed, while no site visits have occurred, and while, in most cases, not even one review of security documentation has been completed and weaknesses are not known, is it best practices to allow folks to connect to CMS, HHS, IRS, and DHS, or was this an extraordinary exception; and if we go back and review another 10 years of documentation we are likely not to see anything else like this again? Can you? Because you are the experts.

Mr. CHAREST. I have not seen it before, sir.

Mr. WOODALL. Ms. Fryer?

Ms. FRYER. And, again, it is best practices, and I know CMS had baseline secure requirements in place for the State. Again, I can't speak to, you know——

Mr. WOODALL. Now, Mr. Baitman, had you been in this meeting, instead of Mr. Trenkle, at the time, would this have raised red flags for you?

Mr. BAITMAN. Yes. I didn't have the background on this, so I wouldn't be able to answer that. I can say that all decisions involve some degree of risk, and there probably were discussions, as Mr. Charest said, that mitigated that risk.

Mr. WOODALL. I wish we had time to talk about whether October 1 really was a legal deadline or whether it was just a politically desirable deadline, and whether we needed to assume those risks on behalf of the American people. But as you said earlier, Mr. Baitman, we are going to do more of these rollouts in the future, and whatever we can learn from this one will no doubt make us better next time around. Thank you all for being here.

Mr. CHAFFETZ. [Presiding.] I thank the gentleman. I now recognize myself for five minutes as we wrap up.

Mr. Baitman, is it accurate that you didn't make a recommendation of a limited launch of Healthcare.gov until after you were aware of significant problems with the development of Healthcare.gov and after you heard of concerns with security testing?

Mr. BAITMAN. I made the recommendation—it wasn't a recommendation, it was a discussion topic, on September 10th, and I hadn't been directly involved. We have a federated structure, so I wasn't directly informed of any specific issues other than——

Mr. CHAFFETZ. Let me keep going. Mr. Baitman, do you, or anybody, ever recall a time when an ATO was elevated to an administrator of an agency because both the chief information security officer and the chief information officer refused to sign the ATO?

Mr. BAITMAN. I am not aware of any.

Mr. CHAFFETZ. Ms. Fryer?

Ms. FRYER. No, sir.

Mr. CHAFFETZ. Mr. Charest?

Mr. CHAREST. I am not aware either.

Mr. CHAFFETZ. Do any of you ever recall reviewing an ATO that did not list a single specific security that was identified by the security control assessment? Anybody ever recall that?

Mr. CHAREST. I am sorry, sir, I am not sure I understand the question.

Mr. CHAFFETZ. Security risk, I should say. Do any of you ever recall reviewing an ATO that listed the main risk for proceeding as a lack of complete security testing? Ms. Fryer?

Ms. FRYER. We do have systems that have indicated that the security testing, there were issues raised during security testing and it is a risk. Normally, it is——

Mr. CHAFFETZ. Any others that were launched without doing the security risk assessment?

Ms. FRYER. No, sir.

Mr. CHAFFETZ. Let me ask you when it was launched, Ms. Fryer, what percentage of the data transfer to the local servers was done over a secure socket layer?

Ms. FRYER. I can't answer that question; I was not involved in the operational day-to-day security and the details of that.

Mr. CHAFFETZ. But you are the chief security officer, are you not? What percentage today of the data transfer is done over a secure socket layer?

Ms. FRYER. Again, that is the operational. I am not involved in the development and implementation of the——

Mr. CHAFFETZ. But you are in charge of the review of it, correct?

Ms. FRYER. I am in charge of the review of the findings during the security control assessment, the independent security control assessments that are conducted, yes.

Mr. CHAFFETZ. Are any of you aware what percentage of the data, when it goes from the computer to the server, is done over a secure socket layer? None of you know the answer to that question? How much of this data that is transferred is encrypted?

Ms. FRYER. The data is encrypted. It is a requirement to be encrypted.

Mr. CHAFFETZ. What percentage of the data is encrypted?

Ms. FRYER. It is encrypted.

Mr. CHAFFETZ. What percentage of it?

Ms. FRYER. It would be 100 percent of the data.

Mr. CHAFFETZ. But you just said you don't know what percentage is done over an SSL.

Ms. FRYER. You are asking what percentage during testing.

Mr. CHAFFETZ. No. I want to know of the actual live site, when somebody in Missouri signs up and they are sending data information, is it all done over an SSL?

Ms. FRYER. They don't send the information over—it depends on if it is a State-based marketplace or they access——

Mr. CHAFFETZ. If you are using Healthcare.gov, is that information encrypted or not?

Ms. FRYER. Yes.

Mr. CHAFFETZ. What percentage of it?

Ms. FRYER. It is encrypted, it is 100 percent.

Mr. CHAFFETZ. Was it on day one?

Ms. FRYER. Yes. That was the requirement to be in place.

Mr. CHAFFETZ. But you don't know what percentage was done over a secure socket layer, which is somewhat similar to saying is it encrypted or not, and you said you didn't know.

Ms. FRYER. Again, I don't know the technology; I am not involved in the operational day-to-day security. I have almost 200 FISMA systems in CMS. That is why we have information——

Mr. CHAFFETZ. So when I have questions about Java script and how you encrypt some of that, you wouldn't know the answer to that.

Ms. FRYER. I know the technical, I don't know of every system in CMS. I don't know the technical——

Mr. CHAFFETZ. We are talking about Healthcare.gov. It is probably the most visible—who does know the answer to that question?

Ms. FRYER. The information systems security officer is the group for the day-to-day development and implementation of secured requirements for Healthcare.gov.

Mr. CHAFFETZ. It scares the living daylights out of me that none of the three of you know the definitive answer about SSLs. If anybody else cares to offer anything, we have a vote on the floor. I am about to close this hearing. Does anybody else have something to offer regarding that point? Listen, we need this stuff to be encrypted, 100 percent of it, 100 percent of the time.

I thank you all for your participation today. This hearing is adjourned.

[Whereupon, at 11:49 a.m., the committee was adjourned.]

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

THE WHITE HOUSE
WASHINGTON

December 15, 2013

The Honorable John Boehner
Speaker
U.S. House of Representatives
Washington D.C. 20515

Dear Speaker Boehner:

I write to raise concerns about the handling of sensitive security testing documents that the House Oversight and Government Reform Committee (HOGR) has subpoenaed from the MITRE Corporation (MITRE). It is the view of cybersecurity experts from across the Administration that these documents, if further disclosed, would provide information to potential hackers that increases the risk they could penetrate healthcare.gov, the Federal Data Services Hub, and other Federal IT systems. In light of our shared interest in cybersecurity across the Federal government, I am seeking your cooperation in ensuring that appropriate procedures are put in place to protect these documents.

Over the past several weeks, both MITRE, the primary security contractor responsible for conducting testing on the healthcare.gov website, and the Department of Health & Human Services (HHS), have explained to HOGR that the security information contained in the documents at issue is highly sensitive. The documents consist of draft and final Security Control Assessments (SCAs) which provide detailed descriptions of the security risks discovered during the regular, legally required assessment of the various components of the Federally Facilitated Marketplace (FFM). As HHS and MITRE security experts have explained to the Committee, the information contained in the assessments provides a roadmap of how to potentially gain unauthorized access to the healthcare.gov website and to manipulate its contents. Even though many of the originally discovered vulnerabilities have been successfully mitigated, details in the unredacted SCAs could be misused to develop a targeted intrusion strategy. In addition, the security assessments provide insight into the FFM system's architecture, including its network and security controls, as well the hardware and software applications it employs. Since many Federal IT systems are built using similar components and techniques, the release of the SCAs for the FFM would increase the ability of sophisticated actors to infiltrate not only the FFM, but potentially other, similarly constructed Federal IT system controls. Finally, given that all Federal IT systems must undergo similar security assessments to certify compliance with the Federal Information Security Management Act (FISMA), public disclosure of these particular SCAs would reduce the utility of all future SCAs, since agencies would face a risk that any identified vulnerabilities would become public.

I understand that both MITRE and HHS have made substantial efforts to arrive at an appropriate accommodation that would satisfy the Committee's oversight interests in light of the above concerns. As part of that process, the Committee was provided several opportunities to further its understanding of the security of the healthcare.gov website and the risks identified in the security assessments consistent with the Executive Branch's interest in protecting the materials from further disclosure:

- On November 6, 2013, the Committee was provided redacted copies of the security documents, which it was able to use in subsequent interviews with agency officials.
- On December 3, 2013, the leader of the MITRE team that conducted the most recent SCA participated in a phone briefing with HOGR staff.
- On December 6, 2013, HHS allowed Committee staff to examine and take notes of unredacted copies of the documents *in camera* at the agency on the condition that any notes would be maintained in a secure location.

In addition, on December 12, HHS sent a letter to HOGR offering a number of additional accommodations, including:

- Providing the unredacted documents in a secure reading room at the Committee's offices;
- Allowing the Committee to invite an independent security expert to inspect the unredacted documents *in camera*;
- Making the unredacted documents available for the Committee to use during interviews with agency officials;
- Offering a briefing on the security documents with HHS cyber-security experts.

To be clear, at no point did HHS suggest that it was unwilling to share this sensitive security information with the Committee, or to discuss potential security risks associated with the healthcare.gov website. However, the Committee Chairman did not respond to any of HHS's proposals, nor did he make any reciprocal effort to find an alternative accommodation. Rather, the Committee Chairman insisted on physical production of the documents without agreeing to put in place any safeguards to ensure their confidentiality.

Following MITRE's production of the unredacted SCAs on December 13, 2013, Secretary Sebelius requested a meeting with Chairman Issa and Ranking Member Cummings to reiterate the grave security concerns associated with further disclosure of these documents and to discuss a protocol for protecting them. I understand that the Secretary's invitation was refused, and it was suggested that the meeting was unnecessary because the Committee knew how to handle sensitive security material. This continued refusal to engage with the Administration is of great concern, particularly in light of the Committee's demonstrated record of disclosing sensitive documents in connection with a number of its investigations and the Chairman's public

assertions that the Committee is not obligated to protect confidential Executive Branch documents such as those at issue here.

I trust that you are as committed as I am to protecting the security of our Federal IT systems and, therefore, I ask that you convene a meeting with Chairman Issa and appropriate representatives of the Administration to discuss the proper protocols that should be put in place by the Chairman to safeguard the sensitive security information in these documents.

Sincerely,

Kathryn H. Ruemmler

Kathryn H. Ruemmler
Counsel to the President

cc: The Honorable Nancy Pelosi
Democratic Leader
U.S. House of Representatives

The Honorable Darrell Issa
Chairman
Committee on Oversight and Government Reform

The Honorable Elijah Cummings
Ranking Minority Member
Committee on Oversight and Government Reform

December 17, 2013

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

Dear Madam Secretary:

The Committee recently obtained results of security assessments of HealthCare.gov conducted by the MITRE Corporation. These documents show a disturbing lack of judgment by HHS officials, who decided to go forward with the launch of HealthCare.gov despite warnings of security vulnerabilities that placed sensitive information of website users at risk. The documents also contradict your public statements that, "when there have been issues identified or flagged, it's immediately fixed.[1]"

While I am withholding sensitive technical details, one security finding summary states, "Any malicious user having knowledge of this can perform unauthorized functions."[2] The summary of another discusses a system weakness that makes a particular type of sensitive information vulnerable. Part of the finding states this, "increases the risk that they will be captured by an attacker."[3] A third, which the document indicates HHS was supposed to address in the days immediately before launch, "The attacker is able to see and edit PII of the victim …"[4]

Adding to our concern, MITRE repeatedly emphasizes in its October 11th final report on its Security Control Assessment (SCA) of the Health Insurance exchange (HIX), that it was forced to omit significant portions of the HIX from its assessment, largely because the project was incomplete. According to MITRE's "Final Report" on the security of HealthCare.gov, dated October 11, 2013:[5]

---

[1] Kelli Kennedy, *Health website remains a work in progress*, AP (Nov. 19, 2013), http://news.yahoo.com/health-website-remain-progress-231249166--finance.html.
[2] HEALTH INSURANCE EXCHANGE (HIX) AUGUST-SEPTEMBER 2013 SECURITY CONTROL ASSESSMENT (Oct. 11, 2013).
[3] *Id.*
[4] *Id.* Note: "PII" is an acronym for "Personally Identifiable Information."
[5] *Id.*

> **1.4 SUMMARY OF ASSESSMENT**
>
> The August and September 2013 assessments of the HIX did not assess functionally complete versions of the Eligibility & Enrollment (E&E), Financial Management (FM), and Plan Management (PM) modules in the same environments. Documentation provided divulged some known functional limitations and omissions due to the software still being developed. The provided lists omitted numerous issues that required investigation to resolve. Workarounds to the components being tested were provided that impacted end to end MITRE test cases.
>
> MITRE was unable to adequately test the Confidentiality and Integrity of the HIX system in full. The majority of the MITRE's testing efforts were focused on testing the expected functionality of the application. Complete end to end testing of the HIX application never occurred. Several factors contributed to the limited effectiveness of this SCA.

While I intend to continue to consult with appropriate security experts before making any decisions about the public release of any specific technical information contained in the MITRE documents, the American people have a right to know the risks they face on HealthCare.gov when they submit sensitive personal information such as their social security number and income. The full context of MITRE's assessment, which the Department had in its possession prior to the October 1 launch date, shows that CMS and HHS knew that HealthCare.gov was vulnerable yet your statements have not given the American people a fair and accurate assessment of known risks.

Of the 28 separate security vulnerabilities identified in the October 11 report, MITRE reported that 19 remained unaddressed. Among the unaddressed security risks that went live on October 1, MITRE indicated eleven "will significantly impact the confidentiality, integrity and/or availability of the system or data...." if the technical or procedural vulnerability is exploited.[6] For others, MITRE defined a risk as "closed" based on upon "the assumption and assurances from CMS" that the risk will be remediated.[7]

While the Committee takes its responsibility to safeguard sensitive technical details about vulnerabilities seriously, we also have a responsibility to inform Americans about the risks they face on HealthCare.gov and to investigate the decision to launch on October 1, 2013, despite serious vulnerabilities and incomplete testing. Contrary to the assertion made by the White House, neither I nor anyone on my staff has expressed an unwillingness to meet with you for a discussion about both the ongoing security vulnerabilities noted in the MITRE documents as well as the rationale for proceeding on October 1, 2013. Indeed, my staff repeatedly has told your staff that it would welcome a page by page discussion of the MITRE documents and any concerns about the public release of any information once the documents were properly and fully produced to the Committee.

---

[6] *Id.*
[7] *Id.*

While I was scheduled to be in my Congressional District office this week, I am willing and prepared to meet with you in my Washington office either today, or tomorrow, Wednesday December 18, to discuss both of our concerns. Please contact my Committee Staff Director Larry Brady to setup a time for this meeting.

Sincerely,

Darrell Issa
Chairman

cc: The Honorable Elijah Cummings, Ranking Minority Member

Brayton, Kathy

From: Blackwood, Kristine (HHS/ASL) [Kristine.Blackwood@hhs.gov]
Sent: Wednesday, January 15, 2014 3:09 PM
To: Grooms, Susanne Sachsman; Marin, Mark; Blase, Brian
Cc: Rapallo, Dave; Brady, Larry
Subject: RE: Classified briefing

If it's a go, please let me know the person at House Security who needs to receive the clearances of the people attending from HHS. Is it Bill McFarland?

From: Grooms, Susanne Sachsman [mailto:Susanne.Grooms@mail.house.gov]
Sent: Wednesday, January 15, 2014 2:17 PM
To: Blackwood, Kristine (HHS/ASL); Marin, Mark; Blase, Brian
Cc: Rapallo, Dave; Brady, Larry
Subject: Re: Classified briefing

Adding Dave and Larry.

We just spoke to the Ranking Member about this, and he thinks it is a good idea. We also contacted House Security and they said they can accommodate this briefing in the CVC at this time.

Brian, I understand Mark is out of the office, but House Security may need a letter to make this happen. We obviously would have to let our members know as well. I'm on my cell if you would like to discuss- 202-570-1345.

Thanks,
Susanne

From: Blackwood, Kristine (HHS/ASL) [mailto:Kristine.Blackwood@hhs.gov]
Sent: Wednesday, January 15, 2014 01:54 PM
To: Marin, Mark; Blase, Brian; Grooms, Susanne Sachsman
Subject: Classified briefing

Dear Mark, Brian, and Susanne,

In advance of the Committee's hearing tomorrow, we wanted to offer your Members and cleared staff the same classified briefing we recently provided to the Energy & Commerce majority and minority Members. The briefing would cover the security incidents that have occurred with respect to the HealthCare.gov website to date, which were covered in the E&C briefing. The CISO security professional doing the briefing on the incidents could also cover issues related to the handling of the type of sensitive IT security information and material the Committee has been receiving, which has been of interest as well.

The classification level required is TS-SCI for certain portions of the briefing. Although I realize it is short notice, we were hoping that this could occur at 8:15 am tomorrow, before the hearing starts, so your Members could attend. We think the briefing will be helpful.

Would you please let me know if this is feasible and of interest to the Committee? If so, we'll bring the briefers to the CVC SCF early tomorrow.

Thanks very much!

Kristine

Kristine Blackwood
Oversight & Investigations
Office of the Assistant Secretary for Legislation
U.S. Department of Health and Human Services
Kristine.Blackwood@HHS.Gov
(202) 690-7627

January 15, 2014

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

Dear Madam Secretary:

At 1:55 p.m. today my staff received an email from Kristine Blackwood, a legislative affairs employee at HHS, offering a classified briefing at 8:15 a.m. tomorrow prior to our hearing which is scheduled to begin at 9:30 a.m.[1] In this e-mail, Ms. Blackwood indicated that this briefing would be similar to one given previously to Members of the House Energy and Commerce Committee.[2]

I would remind you that on December 23, 2013, your staff stated in an e-mail to my Committee Staff Director that your agency would contact our Committee last week – the week of January 6, 2014 – to arrange a meeting to discuss these issues.[3] Despite the commitment to follow-up last week, we never heard from your agency until earlier today when we received the last minute briefing offer for tomorrow morning.[4] We have not received any explanation about why your agency failed to meet its commitment -- or even any notice that it would not be met. We notified the Department of this hearing last week.

Underscoring the scheduling challenge for such a briefing, we also received a letter from your staff today objecting to the Committee's letter of invitation to Frank Baitman, HHS's Chief Information Officer, to testify at our hearing tomorrow.[5] HHS's letter stated "…we believe that this request [to Mr. Baitman to testify at the Committee's hearing] is unreasonable and inappropriate given the 36 hour notice …."[6] On one hand, HHS believes it is unreasonable for the Committee to request the testimony of HHS's Chief Information Officer on 36 hours notice,

[1] Email from Kristine Blackwood to Committee staff, January 15, 2014.
[2] *Id.*
[3] E-mail from Jim Esquea, Assistant Secretary for Legislation at the Department of Health and Human Services, to Committee staff, December 23, 2013.
[4] Email from Kristine Blackwood to Committee staff, January 15, 2014.
[5] Letter from Jim Esquea, Assistant Secretary for Legislation at the Department of Health and Human Services to Darrell Issa, Chairman of the Committee on Oversight and Government Reform.
[6] *Id.*

yet you propose a Committee briefing – for multiple elected officials in a secure environment-- on 18 hours notice.

While we are interested in information about security incidents surrounding HealthCare.gov, given this short notice and HHS's broken scheduling commitments, it is not feasible to schedule this last minute briefing request for tomorrow that your agency was supposed to have proposed last week.

I would also like to remind you that in December I cut short my trip to my California District to meet with you after the White House indicated that you wanted to meet with me to discuss the security issues associated with Healthcare.gov. Despite my acceptance of your invitation, you choose not to meet with me to discuss these matters. While I remain interested in your Department's perspective, I am concerned that the pattern of incompetence and broken commitments Americans have seen in the botched rollout of HealthCare.gov appears to extend to your Department's legislative outreach efforts.

I can only hope that your concerns about the handling of sensitive documents are sincere and not just a ploy intended to distract from a serious discussion with your agency's security experts about bypassed objections to the launch of HealthCare.gov scheduled for tomorrow. My staff will follow-up with your staff to continue our efforts to schedule a workable time and date.

Sincerely,

Darrell Issa
Chairman

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

○