A ROADMAP FOR HACKERS?—DOCUMENTS DETAILING HEALTHCARE.GOV SECURITY VULNERABILITIES

HEARING

BEFORE THE

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED THIRTEENTH CONGRESS

SECOND SESSION

JANUARY 28, 2014

Serial No. 113–141

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

90–891 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

A ROADMAP FOR HACKERS?—DOCUMENTS DETAILING HEALTHCARE.GOV SECURITY VULNERABILITIES

Tuesday, January 28, 2014

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

The committee met, pursuant to call, at 10:05 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, Massie, Collins, Meadows, Bentivolio, DeSantis, Cummings, Maloney, Norton, Tierney, Lynch, Cooper, Connolly, Speier, Cartwright, Duckworth, Davis, and Lujan Grisham.

Staff Present: Brian Blase, Senior Professional Staff Member; Molly Boyl, Deputy General Counsel and Parliamentarian; Lawrence J. Brady, Staff Director; Joseph Brazauskas, Counsel; Daniel Bucheli, Assistant Clerk; Caitlin Carroll, Press Secretary; Sharon Casey, Senior Assistant Clerk; John Cuaderes, Deputy Staff Director; Adam P. Fromm, Director of Member Services and Committee Operations; Linda Good, Chief Clerk; Meinan Goto, Professional Staff Member; Tyler Grimm, Senior Professional Staff Member; Ryan M. Hambleton, Senior Professional Staff Member; Frederick Hill, Deputy Staff Director for Communications and Strategy; Christopher Hixon, Chief Counsel for Oversight; Michael R. Kiko, Legislative Assistant; Mark D. Marin, Deputy Staff Director for Oversight; Ashok M. Pinto, Chief Counsel, Investigations; Laura L. Rush, Deputy Chief Clerk; Sarah Vance, Assistant Clerk; Peter Warren, Legislative Policy Director; Rebecca Watkins, Communications Director; Tamara Alexander, Minority Counsel; Susanne Sachsman Grooms, Minority Deputy Staff Director/Chief Counsel; Jennifer Hoffman, Minority Communications Director; Chris Knauer, Minority Senior Investigator; Julia Krieger, Minority New Media Press Secretary; 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 principles. First of all, Americans have a right to know what they get

from their government and how the money is spent. And second, they deserve an efficient, effective government that works for them.

Our duty on the Oversight and 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. Our job is to work tirelessly, in partnership with citizen watchdogs, to deliver the facts to the American people and bring genuine reform to the Federal bureaucracy.

Before I make my opening statement, it is the chair's intent to go into an executive session in order to protect any items that may be disclosed as to vulnerabilities of the Web site that as of today may or may not have been fully mitigated. So I would advise all staff, members, and the audience that once we go into executive session, we will only have cleared personnel. For members it means stay here. For staff what it means is that you will be asked to leave the room, go back out, sign back in, and be recorded as here.

Additionally, there are numbered packets for information here at your desk. I would admonish all members that these documents are not to be removed. They are committee documents, but they are not personal documents. So you may use them and read them here during the session, they will be available to members and designated staff, but not to be removed. No copies are to be made, and they are not to be removed.

Lastly, these are unclassified documents. They have absolutely no protection under classification to our knowledge. Notwithstanding that, it is our obligation to treat these as potentially sensitive until on a committee basis we are quite comfortable that release would have no adverse effect on the ability of the Web sites to remain up and unhacked.

If there are any questions prior to going to executive session, members may ask them, but I advise that they ask staff beforehand so that we not waste anyone's time, since this is not an ordinary procedure, but a necessary procedure.

I will now recognize myself for an opening statement.

Today's hearing will focus on several remaining questions surrounding the security of HealthCare.gov. In particular, what security risks and concerns were present when the Obama administration decided to launch HealthCare.gov on October 1st; what is being done to fix the critical security risk Web site users are potentially still facing; and what limitations are there on the latest security testing?

When Americans submit their sensitive personal information to HealthCare.gov or, I might add, when government takes sensitive information, including your IRS information, and makes it available through a Web site to outsiders, they deserve to know that it is safe from hackers, bad actors, and security glitches. The possibility of security breach is not some vague, distant concern. It is a real and tangible threat that could affect millions. Private companies devote entire departments to bolstering their online security. They understand the threat of cyber attack is always present and that the consequences of a successful cyber attack can be devastating.

Sadly, the recent security breach at Target, Neiman Marcus, and other companies which have resulted in millions of Americans having their credit card information compromised is an illustration of just how dangerous an attack can be.

The Department of Health and Human Services has repeatedly assured the American public that their sensitive, personally identifiable information transmitted by HealthCare.gov is safe and secure, but because officials authorized the launch of the Web site full of functional errors, Americans have deep skepticism that the site was, in fact, secure. Indeed, documents obtained by this committee by subpoena, around the Health and Human Services, in spite of our repeated attempts to get the information from its source at Health and Human Services, help the committee show that why stopping—security officials at CMS had recommended this site be delayed, not launched, or launched only in part, but CMS officials went ahead anyway, and it is clear that they knew the risk.

Under current law it is possible to launch a site by simply saying that an executive within the administration of the right level has the ability to accept the risk. That current law allows an administration official to accept the risk or almost the assurance that American people's personal identifiable information will be compromised. There is no protection against a judgment call that the risk of billions of dollars, trillions of dollars, the entire economy can, in fact, be waived by an administration official, meaning there is no standard other than the acceptance of risk.

Moreover, 11 weeks after the site is launched, no independent security testing was conducted. Contrary to statements made by Secretary Sebelius at a congressional hearing, independent security testing did not resume until December 9, 2013. When testing did resume, MITRE, the contractor performing the testing, was unable to test half of the functions of the Web site.

Even with the limited scope of testing, MITRE found a high risk that allowed users to access system documents belonging to other users, which could result in the exposure of privileged information to unauthorized individuals. MITRE Corporation found other serious vulnerabilities that would threaten users of HealthCare.gov which have not been shown to the public. These vulnerabilities only reinforce the need for answers, which I intend to pursue.

Since December 15, when the administration offered a meeting with Secretary Sebelius and I flew back during a district work period, I have repeatedly tried to have HHS engage this committee to discuss the security testing documents. I even went so far, again I say, as to fly back to D.C. during the Christmas recess just to meet with Secretary Sebelius. Once back, even though she was in town, she declined for 2 days in a row to offer a meeting time, instead offering a junior level staff briefing.

Until this point, the administration had not made a good faith effort to facilitate a meeting. However, I am pleased that HHS has sent a knowledgeable representative here today so that we can finally have at least the beginnings of a conversation. We are joined today by a top information security officer at the Department of Health and Human Services, as well as an official from MITRE, the company hired by Health and Human Services to conduct the

security control assessments of HealthCare.gov and its many components.

Again, because of the sensitive nature of the security testing documents, we have handled them carefully to ensure sensitive technical information does not end up in the wrong hands, and I will insist that our colleagues continue to respect that.

I must, in closing, share with the American people a personal sensitivity. I believe these documents do reflect ongoing potential loss of personally identifiable information belonging to the American people. However, if I am to take the administration at their word, there are no vulnerabilities unmitigated. Therefore, these documents are not a hacker's access to your personal information, and yet, when asking for briefings, I get told that they have to be closed and in fact that these documents cannot be released.

The administration cannot have it both ways. They can't both say these documents represent completely mitigated vulnerabilities and then say, but they are a pathway, so they can't be released. It is this committee's intent to err on the side of the assumption that the administration continues to lie about the site being safe and secure. We can find no other basis but to assume that they were lying about the vulnerabilities on the day they went live on October 1st and that they are still lying.

I don't use the word lie without real forethought. You cannot continue to tell people there is no problem; there was a problem on October 1st. You cannot tell people they have been mitigated, and then tell them, but don't release the documents because it is a pathway for hackers.

So I will assume that the truth is the site was vulnerable on launch date, they went ahead with known vulnerabilities, and that they continue to have unknown areas that could cause information to be made available outside of those having a right to. We can take no other assumptions. I hope in the long run we find that it was far less than it appeared to be. But with that I recognize Mr. Cummings for his opening statement.

Mr. CUMMINGS. Thank you very much, Mr. Chairman. And I hope that our witnesses can shed some light on the many lies that you allege have been told.

Today is the 23rd hearing our committee has held on the Affordable Care Act. As I did at our previous hearing 2 weeks ago, I want to recognize the importance of what has been accomplished for the American people. And when I say the American people, I mean both Republican and Democrat, I mean all of America.

The law went into full effect on January 1st, and now millions of people are obtaining health insurance coverage they did not have before. Some of them have never had healthcare insurance. They are receiving critical medical care, and they have the security of knowing they will not go bankrupt if they get into an accident or get sick. This is, without a doubt, a historic achievement.

The law also put into place key protections for consumers. Insurance companies are now prohibited from discriminating—that is what I said, discriminating—against people with cancer, diabetes, heart disease, and preexisting conditions. Again, I am talking about our constituents, Americans, the ones who pay taxes and work hard every day. Insurance companies may not charge higher

prices for women, and millions of people are now receiving free preventative care. The President has made it clear that he wants to keep people well because it is far cheaper to keep them 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 health care costs in 50 years. If we repeal the law today, it would increase our deficit by more than 1.5 trillion—not billion—trillion dollars.

In terms of the security of the Web site, we received testimony just 2 weeks ago from chief information security officer of the CMS. She told us, and I quote, "There have been no successful security attacks on the FFM, and no person or group has maliciously accessed personally identifiable information," end of quote. I want to repeat that: No person or group has maliciously accessed personally identifiable information on the HealthCare.gov Web site.

The chief information security officer also said that following security testing in December, HealthCare.gov has, and I quote, "a clean bill of health," end of quote.

Although no system is hack-proof, she said she is and I quote, "confident based on the recent security controls assessment and the additional security protections in place that the FFM is secure," end of quote.

I want to thank the chairman for proposing that today's hearing be held in executive session, a motion that I fully support. The MITRE Corporation and the Department of Health and Human Services have warned the committee repeatedly that some of the security testing documents we have obtained contain highly sensitive information and can provide a road map for hackers and others seeking to do us harm. I think it is a positive step that the committee is willing to hear from these officials firsthand about their concerns. Conducting the hearing in executive session will allow us to discuss this sensitive information directly with the experts.

As we have heard on numerous occasions from the cybersecurity experts at MITRE and the Department, the security control assessments contain information about cybersecurity methods and the fundamental cyber architecture of HealthCare.gov that, and I quote, "transcends the specific security control vulnerabilities which have been the focus of news reports and the committee's public inquiry," end of quote. Even when specific vulnerabilities identified by security testing have been addressed, these experts warn that publicly disclosing the security control assessments could still jeopardize HealthCare.gov and other CMS data networks, and again I hope our witnesses will shed light on that since the chairman has alleged that so many people have been lying.

I believe our goal as a committee should be to conduct responsible oversight that provides the American public with information necessary to understand the security of the HealthCare.gov Web site, while at the same time protecting sensitive information that could endanger the Web site's functioning or compromise the personal information of the American people.

Let me conclude by thanking the officials testifying here today.

Dr. Charest, this is your second time before the committee in as many weeks. Thank you for returning to address these vital questions in closed session.

Mr. Shomo, I understand that you are one of the engineers responsible for conducting security testing of HealthCare.gov on behalf of MITRE Corporation, and we thank you for being here.

As a nonprofit organization with a long history of running federally funded research and development programs, MITRE is known and respected for its objectivity and independence. We appreciate everything you both are doing to remain vigilant and protect the security of HealthCare.gov. Millions of American families thank you for helping them to get access to lifesaving care that they so desperately need.

And with that I yield back.

Chairman ISSA. Thank you.

I now ask unanimous consent that the document signed by Marilyn Tavenner, which is the authority to operate, be placed in the record. Without objection, so ordered.

Pursuant to that document, which says that within 60 to 90—I will read it verbatim—conduct a full SCA test on the FFM, including its three modules, E&E, FM, and PM, in a stable environment where all security controls can be tested within 60 to 90 days of going live on October 1st.

Based on this document, which declares known vulnerabilities that must be tested and mitigated within 60 to 90 days, I now recognize the gentleman from Florida for a motion.

Mr. MICA. Mr. Chairman, so the Committee on Oversight and Government Reform may proceed in executive session and continue its business pursuant to House Rule XI(g)(2), I move that the remainder of the hearing be closed to the public because the disclosure of the testimony to be heard may compromise sensitive law enforcement information.

Chairman ISSA. The question is on agreeing to the motion to close the hearing. The clerk will call the roll.

The CLERK. Mr. Issa?

Chairman ISSA. Yea.

The CLERK. Mr. Issa votes aye.

Mr. Mica?

Mr. MICA. Aye.

The CLERK. Mr. Mica votes aye.

Mr. Turner?

Mr. TURNER. Aye.

The CLERK. Mr. Turner votes aye.

Mr. Duncan?

Mr. DUNCAN. Aye.

The CLERK. Mr. Duncan votes aye.

Mr. McHenry?

[No response.]

The CLERK. Mr. Jordan?

Mr. JORDAN. Yes.

The CLERK. Mr. Jordan votes aye.

Mr. Chaffetz?

Mr. CHAFFETZ. Aye.

The CLERK. Mr. Chaffetz votes aye.

Mr. Walberg?
Mr. WALBERG. Aye.
The CLERK. Mr. Walberg votes aye.
Mr. Lankford?
Mr. LANKFORD. Yes.
The CLERK. Mr. Lankford votes aye.
Mr. Amash?
Mr. AMASH. Yes.
The CLERK. Mr. Amash votes aye.
Mr. Gosar?
Mr. GOSAR. Yes.
The CLERK. Mr. Gosar votes aye.
Mr. Meehan?
Mr. MEEHAN. Aye.
The CLERK. Mr. Meehan votes aye.
Mr. DesJarlais?
Mr. DESJARLAIS. Aye.
The CLERK. Mr. DesJarlais votes aye.
Mr. Gowdy?
Mr. GOWDY. Yes.
The CLERK. Mr. Gowdy votes aye.
Mr. Farenthold?
Mr. FARENTHOLD. Yes.
The CLERK. Mr. Farenthold votes aye.
Mr. Hastings?
[No response.]
The CLERK. Mrs. Lummis?
[No response.]
The CLERK. Mr. Woodall?
[No response.]
The CLERK. Mr. Massie?
Mr. MASSIE. Aye.
The CLERK. Mr. Massie votes aye.
Mr. Collins?
Mr. COLLINS. Aye.
The CLERK. Mr. Collins votes aye.
Mr. Meadows?
Mr. MEADOWS. Aye.
The CLERK. Mr. Meadows votes aye.
Mr. Bentivolio?
Mr. BENTIVOLIO. Aye.
The CLERK. Mr. Bentivolio votes aye.
Mr. DeSantis?
Mr. DESANTIS. Aye.
The CLERK. Mr. DeSantis votes aye.
Mr. Cummings?
Mr. CUMMINGS. Yes.
The CLERK. Mr. Cummings votes aye.
Mrs. Maloney?
Mrs. MALONEY. Aye.
The CLERK. Mrs. Maloney votes aye.
Ms. Norton?
[No response.]
The CLERK. Mr. Tierney?

Mr. TIERNEY. Aye.
The CLERK. Mr. Tierney votes aye.
Mr. Clay?
[No response.]
The CLERK. Mr. Lynch?
Mr. LYNCH. Aye.
The CLERK. Mr. Lynch votes aye.
Mr. Cooper?
Mr. COOPER. Aye.
The CLERK. Mr. Cooper votes aye.
Mr. Connolly?
[No response.]
The CLERK. Ms. Speier?
[No response.]
The CLERK. Mr. Cartwright?
Mr. CARTWRIGHT. Aye.
The CLERK. Mr. Cartwright votes aye.
Ms. Duckworth?
Ms. DUCKWORTH. Aye.
The CLERK. Ms. Duckworth votes aye.
Ms. Kelly?
[No response.]
The CLERK. Mr. Davis?
Mr. DAVIS. Aye.
The CLERK. Mr. Davis votes aye.
Mr. Welch?
[No response.]
The CLERK. Mr. Cardenas?
[No response.]
The CLERK. Mr. Horsford?
[No response.]
The CLERK. Ms. Lujan Grisham?
[No response.]
Chairman ISSA. The clerk will report the tally.
The CLERK. Twenty-seven ayes, zero noes.

Chairman ISSA. There being 27 ayes and zero noes, the motion is agreed to. The clerk will now clear the room. Only Members of Congress, cleared staff, the witnesses, and their cleared counsels may remain in the hearing room. The committee stands in a short recess.

[Whereupon, at 10:27 a.m., the committee proceeded to closed session.]

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

DATE:

TO: Marilyn Tavenner

FROM: James Kerr, Consortium Administrator for Medicare Health Plans Operations
Henry Chao, Deputy Chief Information Officer & Office of Information Services Deputy Director

SUBJECT: Federally Facilitated Marketplace–DECISION

ISSUE:

The Federal Information Security Management Act (FISMA) requires that the various Federally Facilitated Marketplace (FFM) systems - Enterprise and Eligibility (E&E), Financial Management (FM), and Plan Management (PM) successfully undergo a Security Control Assessment (SCA). Due to system readiness issues, the SCA was only partly completed. This constitutes a risk that must be accepted and mitigated to support the Marketplace Day 1 operations.

BACKGROUND:

CMS utilizes independent and specialized contractors to test the security readiness of its systems. Testing of the Marketplace has been on-going since inception as part of the CMS Expedited Life-Cycle process with the latest security testing occurring in September of 2013. As with all new systems which are pending launch, there are inherent security risks with not having all code tested in a single environment, finally, the system requires rapid development and release of hot-fixes and patches so it is not always available or stable during the duration of testing,

From a security perspective, the aspects of the system that were not tested due to the ongoing development, exposed a level of uncertainty that can be deemed as a high risk for FFM. Although throughout the three rounds of SCA testing all of the security controls have been tested on different versions of the system, the security contractor has not been able to test all of the security controls in one complete version of the system.

The risk associated with issuing an ATO for the FFM will be reduced by instituting a two-part mitigation plan.

First, CMS will implement the following security processes for the first year of operation of FFM:

- Establish a dedicated security team under the Chief Information Officer (CIO) to monitor, track and ensure the mitigation plan activities are completed. The CIO and the Chief Information Security Officer (CISO) will report weekly on the progress to the Health Reform Operations Board;

Page 2 – The Administrator

- Monitor and perform weekly testing of all border devices, including internet facing web servers;
- Conduct daily/weekly scans using the CISO's continuous monitoring tools
- Conduct a full SCA test on FFM (E&E, FM and PM) in a stable environment where all security controls can be tested within 60/90 days of going live on October 1st.

Second, CMS will migrate the Marketplace systems to CMS' Virtual Data Center (VDC) environment in Q1-2014. This environment has been through a full security assessment and has an authority to operate.

RECOMMENDATION:

Issue an Authority-to-Operate (ATO) for six months and implement the mitigation plan. The six-month period will allow the Marketplace to normalize its development activities while enabling the security team to closely monitor activities and perform a complete SCA.

DECISION:

Approved Marilyn Tavenner Date SEP 27 2013

Disapproved _____ Date _____

Marilyn Tavenner

Attachment: Federally Facilitated Marketplace Decision Memo Risk Acknowledgment Signature Page

DEPARTMENT OF HEALTH & HUMAN SERVICES
Centers for Medicare & Medicaid Services
7500 Security Boulevard, Mail Stop
Baltimore, Maryland 21244-1850

CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES

Federally Facilitated Marketplace Decision Memo
Risk Acknowledgment Signature Page

We acknowledge the level of risk the Agency is accepting in the Federally Facilitated Marketplace (FFM). The mitigation plan does not reduce the risk to the FFM system itself going into operation on October 1, 2013. However, the added protections do reduce the risk to the overall Marketplace operations and will ensure that the FFM system is completely tested within the next 6 months.

Reviewer Teresa Fryer (Teresa Fryer) Date 9-27-2013

Reviewer Tony Trenkle (Tony Trenkle) Date 9-27-2013

Reviewer Michelle Snyder (Michelle Snyder) Date 9-27-2013