

DARRELL E. ISSA, CALIFORNIA  
CHAIRMAN

JOHN L. MICA, FLORIDA  
MICHAEL R. TURNER, OHIO  
JOHN J. DUNCAN, JR., TENNESSEE  
PATRICK T. MCHEERY, 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

ONE HUNDRED THIRTEENTH CONGRESS

# Congress of the United States

## House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5074

FACSIMILE (202) 225-3974

MINORITY (202) 225-5051

<http://oversight.house.gov>

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  
MARK POCAN, WISCONSIN  
L. 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

LAWRENCE J. BRADY  
STAFF DIRECTOR

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."<sup>1</sup>

While I am withholding sensitive technical details, one security finding summary states, "Any malicious user having knowledge of this can perform unauthorized functions."<sup>2</sup> 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."<sup>3</sup> 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 ..."<sup>4</sup>

Adding to our concern, MITRE repeatedly emphasizes in its October 11<sup>th</sup> 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:<sup>5</sup>

<sup>1</sup> Kelli Kennedy, *Health website remains a work in progress*, AP (Nov. 19, 2013), <http://news.yahoo.com/health-website-remain-progress-231249166--finance.html>.

<sup>2</sup> HEALTH INSURANCE EXCHANGE (HIX) AUGUST-SEPTEMBER 2013 SECURITY CONTROL ASSESSMENT (Oct. 11, 2013).

<sup>3</sup> *Id.*

<sup>4</sup> *Id.* Note: "PII" is an acronym for "Personally Identifiable Information."

<sup>5</sup> *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.<sup>6</sup> For others, MITRE defined a risk as "closed" based on upon "the assumption and assurances from CMS" that the risk will be remediated.<sup>7</sup>

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.

---

<sup>6</sup> *Id.*

<sup>7</sup> *Id.*

The Honorable Kathleen Sebelius

December 17, 2013

Page 3

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,

A handwritten signature in blue ink, appearing to read "Darrell Issa", with a stylized flourish at the end.

Darrell Issa  
Chairman

cc: The Honorable Elijah Cummings, Ranking Minority Member