

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

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
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
VACANCY

LAWRENCE J. BRADY
STAFF DIRECTOR

March 25, 2014

The Honorable John W. Hickenlooper
Governor of Colorado
136 State Capitol
Denver, CO 80203-1792

Dear Governor Hickenlooper:

Over the past four years, the Committee on Oversight and Government Reform has been conducting oversight of the Obama Administration's implementation of ObamaCare. We are writing to you because the Committee has learned that the Obama Administration took actions in the summer and fall of 2013 that appear to have placed the private information of Colorado residents at risk with the launch of ObamaCare's health insurance exchanges. We write to provide you with information pertinent to the citizens of your state as well as to request your assistance with the Committee's ongoing oversight.

Independent Security Assessment of Colorado's Exchange Raised Security Concerns

Since October 1, 2013, Americans in states with exchanges established by the federal government have been entering their personally identifiable information (PII), such as birth dates, Social Security numbers, and income as well as PII of family members into HealthCare.gov. Individuals in states that established state health insurance exchanges, including Colorado, have likewise been entering this information into similar websites. Federal agencies, including the Internal Revenue Service and the Social Security Administration, have responsibility for verifying much of the information provided by individuals applying for coverage through the exchanges. The information provided by these agencies passes through the federal data services hub to the ObamaCare exchanges, where the information is then stored.¹

In September 2013, Colorado contracted with Coalfire Systems Inc. to conduct an independent security assessment of its exchange as required by the Centers for Medicare and

¹ Department of Health and Human Services, Office of Inspector General, Observations Noted During the OIG Review of CMS's Implementation of the Health Insurance Exchange—Data Services Hub (Aug. 2013), <https://oig.hhs.gov/oas/reports/region1/181330070.pdf>.

Medicaid Services (CMS) Minimum Acceptable Risk Standards for Exchanges (MARS-E).² According to Coalfire, the assessment determined if a sampling of appropriate security controls complied with CMS's requirements, but it was not "a formal CMS Security Control Assessment (SCA) required for system accreditation."³ The Committee is not aware of whether a formal SCA has ever been performed on the Colorado exchange.

Coalfire's assessment raises serious questions about the security of Colorado's exchange when it launched on October 1, 2013. Coalfire found that the exchange satisfied only 56 percent of system security controls and control enhancements as of September 23, 2013.⁴ According to Coalfire's report, several "IRS [Affordable Care Act] critical controls, such as identification and authentication and physical access control, were not satisfied."⁵ Coalfire Systems also assessed the physical security of Colorado's exchange facilities, finding that only 50 percent of those security controls were satisfied.⁶ In its report, Coalfire stated that the exchange "is not yet conformant with the compliance standards and frameworks [of CMS, IRS, or the National Institute for Standards and Technology (NIST).]"⁷ Since Coalfire's security assessment occurred during the end of September, it appears that the Colorado exchange did not comply with CMS, IRS, or NIST standards when it launched on October 1, 2013. It is unclear when, if at all, the numerous deficiencies in the security of Colorado's exchange were corrected.

Obama Administration Allowed Colorado to Connect to Federal Data Hub Despite High Risks

The Committee has recently obtained the security risk assessment of the Chief Information Security Officer (CISO) at CMS for allowing states to connect to the data services hub. State exchanges and Medicaid systems needed authority to connect (ATC) agreements from CMS in order to connect to the federal data services hub.

After its review, the CISO only recommended four state systems be allowed to connect to the hub. According to the reviews, the CISO deemed 35 state systems as a high risk and an additional ten state systems as a moderate risk of connecting to the data hub.⁸ NIST defines a moderate risk as a risk where "the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or

² Centers for Medicare and Medicaid Services, Catalog of Minimum Acceptable Risk Controls for Exchanges – Exchange Reference Architecture Supplement 42-44 (Aug. 1, 2010), *available at*: <http://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/Catalog-of-MinAcceptable-Risk-Controls-for-Exchanges-ERA-Supp-v-1-0-08012012-a.pdf>.

³ *Id.*

⁴ *Id.*

⁵ *Id.*

⁶ *Id.*

⁷ *Id.*

⁸ CMS CISO Reviewer Overall Comments & Recommendations (on file with Committee staff).

individuals”⁹ and a high risk as a risk where “the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.”¹⁰

Despite the CISO’s negative assessments that generally revealed incomplete documentation and inadequate security testing, CMS allowed most of these states to connect to the federal data hub on October 1, 2013. A few days prior to October 1, 2013, Ryan Brewer, CMS’s CISO from 2009 through 2011 and currently an advisor to CMS on information security matters, offered the following assessment to current CMS CISO Teresa Fryer: “Allowing these states to connect to the Hub and FFM [Federally Facilitated Marketplace] without the appropriate review of their documentation introduces an unknown amount of risk to the Hub and FFM. **This in turn puts the PII of potentially millions of users at risk of identity theft and fraud to the CMS marketplace healthcare subsidy program.**”¹¹ [emphasis added]

It does not appear, however, such concerns were welcomed by senior CMS management in the days leading up to the October 1, 2013, launch date. In response to a September 29, 2013, e-mail from Mike Mellor, CMS Deputy CISO, about an ATC “signing party,”¹² Ms. Fryer wrote, “normally I just review and sign what Ryan [Brewer] gives me anyway because **the front office is signing them whether or not they are a high risk.**”¹³ [emphasis added] At the time, CMS’s front office consisted of CMS’s Chief Information Officer Tony Trenkle, CMS’s Deputy Chief Information Officer Henry Chao, and CMS’s Chief Technology Officer George Linares.¹⁴ Ms. Fryer testified that by authorizing states to connect to the data hub CMS accepted “a risk, again, of the unknowns, because things haven’t been tested.”¹⁵

⁹ See U.S. Dep’t of Commerce, Federal Information Process Standards Publication, Standards for Security Categorization of Federal Information and Information Systems, FIPS PUB 199, at 2 (Feb. 2004) (hereinafter “FIPS PUB 199”). According to NIST, a serious adverse effect means that, for example, the loss of confidentiality, integrity or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.

¹⁰ *Id.* at 3. According to NIST, a severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

¹¹ E-mail from C. Ryan Brewer, Principal, GrayScout, LLC, to Teresa M. Fryer, CISO, CMS (Sept. 18, 2013, 2:17 PM) (on file with Committee staff).

¹² E-Mail from Michael Mellor, Deputy CISO, CMS, to Teresa M. Fryer, CISO, CMS (Sept. 29, 2013, 7:02 AM) (on file with Committee staff).

¹³ E-mail from Teresa M. Fryer, CISO, CMS, to C. Ryan Brewer, Principal, GrayScout, LLC, and Michael Mellor, Deputy CISO, CMS (Sept. 29, 2013, 8:15:55 AM) (on file with Committee staff).

¹⁴ Transcribed Interview with Thomas Schankweiler, Information Security Officer, Centers for Medicare and Medicaid Services, in Wash. D.C. (Dec. 17, 2013).

¹⁵ Transcribed Interview with Teresa Fryer, Chief Information Security Officer, Centers for Medicare and Medicaid Services, in Wash. D.C. (Dec. 17, 2013).

On September 29, 2013, CMS's CISO completed its assessment of Colorado's ATC package.¹⁶ The CISO considered several factors in its assessment, including CMS's security experts' review of documentation submitted by the Colorado exchange, CMS's Office of E-Health Standards and Services assessment that Colorado's exchange posed an "unknown risk for Privacy compliance," and the fact that 72 security controls were either not answered or incomplete. Based on this information, the CISO concluded that there was a high risk if CMS allowed Colorado's exchange to connect to the data hub.¹⁷ The CISO recommended several actions Colorado could take to reduce the high risk, but these fixes, if they took place, likely did not occur until after October 1, 2013.¹⁸ Despite the high risk, CMS allowed Colorado's exchange to connect to the data hub on October 1, 2013.

Due to the decision of the Obama Administration to launch the exchanges on October 1, 2013, before states could properly test their systems and government security experts could properly review security documentation and address known problems, the personal information of millions of Americans who have sought to obtain coverage through the exchanges was put at risk. As the Committee continues its oversight of ObamaCare, we request that you provide the following information to the Committee by April 8, 2014.

- 1) All documents and communications between any employees, contractors, or agents of the State of Colorado and any employees, contractors, or agents of the U.S. Department of Health and Human Services, including but not limited to any employees, contractors, or agents of the Centers for Medicare and Medicaid Services, referring or relating to the Colorado exchange or the federal data services hub between May 1, 2013, and the present.
- 2) All documents and communications between any employees, contractors, or agents of the State of Colorado and any employees, contractors, or agents of the White House, including but not limited to the Executive Office of the President, referring or relating to the Colorado exchange or the federal data services hub between May 1, 2013, and the present.
- 3) All assessments or audits of the Colorado exchange's development, readiness, or security between July 1, 2012, and the present.

¹⁶ CISO Reviewer Overall Comments and Recommendations of the Colorado Health Benefit Exchange/Connect for Health (Sept. 29, 2013).

¹⁷ *Id.*

¹⁸ *Id.*

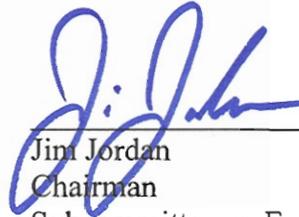
The Honorable John W. Hickenlooper
March 25, 2014
Page 5

The Committee on Oversight and Government Reform is the principal oversight committee of the House of Representatives and has broad authority to investigate “any matter” at “any time” under House Rule X. If you have any questions about this request, please contact Brian Blase or Meinan Goto of the Committee staff at (202) 225-5074. Thank you for your attention to this important matter.

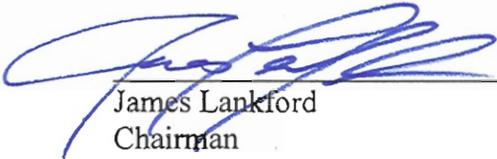
Sincerely,



Darrell Issa
Chairman



Jim Jordan
Chairman
Subcommittee on Economic Growth,
Job Creation, and Regulatory Affairs



James Lankford
Chairman
Subcommittee on Energy Policy,
Health Care and Entitlements

Enclosure

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

The Honorable Matthew A. Cartwright, Ranking Minority Member
Subcommittee on Economic Growth, Job Creation and Regulatory Affairs

The Honorable Jackie Speier, Ranking Minority Member
Subcommittee on Energy Policy, Health Care and Entitlements