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

March 25, 2014

The Honorable Vincent C. Gray
Mayor, District of Columbia
John A. Wilson Building
1350 Pennsylvania Avenue, NW
Washington, D.C. 20004

Dear Mayor Gray:

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 residents of the District of Columbia at risk with the launch of ObamaCare's health insurance exchanges. We write to provide you with information pertinent to the citizens of the District as well as to request your assistance with the Committee's ongoing oversight.

Independent Security Assessment of the District of Columbia'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 the District of Columbia, 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 ObamaCare exchanges. The information provided by these agencies passes through the federal data services hub to the exchanges, where the information is then stored.[1]

[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.

The District of Columbia contracted with SeNet Corporation to conduct an independent security assessment of its exchange as required by the Centers for Medicare and Medicaid Services (CMS) Minimum Acceptable Risk Standards for Exchanges (MARS-E).[2] SeNet conducted this assessment between August 19, 2013, and September 12, 2013.[3] On September 18, 2013, SeNet published its assessment, called the Assessment Report of the District of Columbia Access System Health Benefit Exchange Authority.[4]

SeNet's assessment raises serious questions about the security of the District of Columbia exchange when it launched on October 1, 2013. In the report, SeNet identified 76 total weaknesses, including 19 high risks and 23 moderate risks.[5] The National Institute of Standards and Technology (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 individuals,"[6] 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."[7] Among the risks, SeNet's report described password and log-in vulnerabilities present as of August 28, 2013.[8] According to SeNet, it was easy to break into other users' accounts simply by guessing and cross-referencing a database containing a dictionary.[9] It is unclear when, if at all, the numerous deficiencies in the security of the District of Columbia's exchange were corrected.

---

[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] District of Columbia Access System Health Benefit Exchange Authority Security Assessment Report, at 3 (Sept. 18, 2013) (hereinafter "DCAS Report").

[4] *Id.* at 1.

[5] *Id.* at 9.

[6] *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 or life or serious life threatening injuries.

[7] *See 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.

[8] DCAS Report, *supra* note 2, at 13.

[9] *Id.*

Obama Administration Allowed the District of Columbia 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.[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]

---

[10] CMS CISO Reviewer Overall Comments & Recommendations (on file with Committee staff).
[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 26, 2013, CMS's CISO completed its assessment of the District of Columbia's ATC package.[16] The CISO considered several factors in its assessment, including CMS's security experts' review of documentation submitted by the District of Columbia exchange and CMS's Office of E-Health Standards and Services, which concluded that the District of Columbia's exchange posed a "High risk for Privacy compliance." Based on this information, the CISO concluded that there was a high risk if CMS allowed the District of Columbia's exchange to connect to the data hub.[17] The CISO recommended several actions for ways the District of Columbia could 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 the District of Columbia'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 District of Columbia 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 District of Columbia 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 District of Columbia 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 District of Columbia exchange or the federal data services hub between May 1, 2013, and the present.

3) All assessments or audits of the District of Columbia exchange's development, readiness, or security between July 1, 2012, and the present.

---

[16] CISO Reviewer Overall Comments and Recommendations of the District of Columbia Access System ATC (Sept. 26, 2013).
[17] *Id.*
[18] *Id.*

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