LAMAR S. SMITH, Texas
CHAIRMAN

EDDIE BERNICE JOHNSON, Texas
RANKING MEMBER

Congress of the United States
House of Representatives

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

2321 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515–6301

(202) 225–6371
www.science.house.gov

January 28, 2015

Hon. Marilyn Tavenner
Administrator
Centers for Medicare and Medicaid Services
7500 Security Boulevard
Baltimore, MD 21244

Dear Ms. Tavenner,

According to an *Associated Press* (AP) story published last week,[1] as many as 50 data mining companies were provided direct access to monitor information entered on the HealthCare.gov website. It appears this access was provided with permission and even encouragement from the federal government. Every American who has visited the Obamacare website may have been monitored by numerous companies without their consent or knowledge. This revelation raises serious questions about both personal privacy and cybersecurity on the HealthCare.gov website.

The AP reported that when a person applies for coverage through HealthCare.gov, approximately 50 data mining companies immediately become aware of the individual's online presence. Data mining companies can then search for sensitive personal information that applicants are required to enter. This can include a social security number, annual salary, employment, place of residence, immigration status, military service, criminal history, financial information, age, whether one is pregnant, whether one smokes and more.

Once a data mining company seizes this treasure trove of sensitive personal information, it is able to combine this data with other information collected by tapping into commercial websites and databases such as phone calls, texts, social media posts, frequently visited websites, and credit card purchases. These detailed electronic dossiers on millions of Americans could then be sold to other businesses, U.S. government agencies, foreign governments and even criminal enterprises that are willing to pay large sums of money for the information.

Data mining companies gather and sell personal information without our knowledge or consent. Indeed, one of the branches of the commercial cybersecurity industry focuses on the prevention of data mining. It is astonishing that the Obama administration has allowed scores of these companies to take up permanent residence on the HealthCare.gov website.

A spokesman for the Centers for Medicare and Medicaid Services (CMS) confirmed to AP that outside vendors were allowed on HealthCare.gov in order to provide feedback about website quality and

---

[1] Ricardo Alonso-Zaldivar and Jack Gillum, "New Privacy Concerns Over Government's Health Care Website," AP News, January 20, 2015, available at: http://apnews.myway.com/article/20150120/us--health_overhaul-privacy-8b7c5d925b.html.

user convenience. According to the spokesman, outside vendors "are prohibited from using information from these tools on HealthCare.gov for their companies' purposes."[2] Nevertheless, it isn't clear how, or if, CMS is able to monitor what data mining companies are doing on HealthCare.gov.

Outside cybersecurity experts who commented for the AP story expressed surprise and concern that so many companies are permitted at HealthCare.gov, since website quality control assessments could be handled by just one or two outside firms. Experts pointed out that outside vendors are often the weak link for serious cybersecurity breaches -- like the one that affected Target and millions of its customers. In the case of HealthCare.gov, a cybersecurity breach could threaten all of the federal agencies (e.g., the Internal Revenue Service) as well as the millions of Americans who visit the website.

The Federal Information Security Management Act of 2002 (FISMA) requires all federal agencies to develop and implement programs that secure their information and information systems. Under FISMA, each agency must conduct annual reviews of its information security program, and report the results to the Office of Management and Budget (OMB). OMB, in turn, has FISMA oversight responsibilities and must submit an annual report to Congress.

The National Institute of Standards and Technology (NIST), over which this Committee has jurisdiction, "develops and issues standards, guidelines, and other publications to assist federal agencies in implementing FISMA and in managing cost-effective programs to protect their information and information systems."[3] Each agency's information control system must be reviewed, certified and accredited under NIST publication SP 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems."[4] Security accreditation is required under OMB Circular A-130, Appendix III. Accredited systems must be monitored continuously, including ongoing assessment of security controls. By accrediting an agency's information system, the responsible agency official accepts responsibility for the security of the system and is fully accountable for any adverse impacts to the agency if a breach of security occurs.

Given the Committee's concerns over the privacy of individuals and cybersecurity ramifications of the presence of data mining companies on HealthCare.gov, I would appreciate answers to the following questions by February 6, 2015:

1) Before the AP news story, were you aware of the presence of data mining companies on HealthCare.gov?
2) Were you consulted about the decision to allow this? If not, who was consulted and who authorized this?
3) What is the justification for allowing several dozen data mining companies to inhabit HealthCare.gov and should they be allowed to continue occupying the website?

---

[2] Ibid.
[3] NIST, Information Technology Laboratory, Computer Security Division, Computer Security Resource Center, FISMA Compliance, available at: http://csrc.nist.gov/groups/SMA/fisma/compliance.html.
[4] NIST Special Publication 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems," May 2004, available at: https://www.fismacenter.com/SP800-37-final.pdf.

4) Are you aware of any CMS capability to monitor adequately the activities of the outside firms that are embedded in HealthCare.gov? Are you concerned that some of these companies may be gathering sensitive personal information from the millions of Americans who have applied for health insurance coverage on HealthCare.gov?
5) In your view, is CMS' decision to allow dozens of outside data mining companies on HealthCare.gov consistent with the Federal Information Security Management Act?
6) If CMS is not FISMA compliant for HealthCare.gov, what steps will be taken to achieve compliance and how soon?
7) How many of these private data mining companies have or have had access to the information on HealthCare.gov? In response to this question, please provide a list of all data mining companies on HealthCare.gov, including their specific role and reason for their presence on the website, and authorizations they were given by the government regarding the extent and types of data they could monitor and/or collect on HealthCare.gov, and what they were, or are, permitted to do with that information.
8) Further, please furnish all official communications with the data mining companies that have had access to HealthCare.gov, including with your office, the U.S. Department of Health and Human Services (HHS) and the Office of Science and Technology Policy (OSTP).

The Committee is posing questions similar to those above to OSTP and HHS. In light of the serious issues of personal privacy and government information security raised by the recent news reports, the Committee may ask you to appear on relatively short notice and testify.

If your staff has any questions, please contact Cliff Shannon, Staff Director of the Research and Technology Subcommittee, at Cliff.Shannon@mail.house.gov or (202) 226-9783.

Sincerely,

Lamar Smith
Chairman

cc: Eddie Bernice Johnson
Ranking Member