Congress of the United States

Washington, DC 20510

September 17, 2014

The Honorable Marilyn Tavenner
Administrator
Centers for Medicare & Medicaid Services
200 Independence Avenue, SW
Washington, DC 20201

Re: GAO Report No. 14-730

Dear Administrator Tavenner:

We write to express our concerns and request further information about the security of the HealthCare.gov website. The report released yesterday by the Government Accountability Office (GAO) on HealthCare.gov indicates that mismanagement of the website's development by the Centers for Medicare and Medicaid Services (CMS) has created numerous security vulnerabilities.[1] This report comes just two weeks after CMS announced that a hacker had installed malicious software on a server within the HealthCare.gov network that went undetected for almost two months.[2] Yesterday's report and recent security breaches raise dire concerns about whether Americans can trust HealthCare.gov with their personal and sensitive information.

Since its inception, there have been serious concerns about the security of HealthCare.gov. The website was created by CMS to run the Federally Facilitated Marketplace (FFM) established by the Patient Protection and Affordable Care Act. In order to enroll beneficiaries in the exchange, HealthCare.gov collects, obtains and retains massive amounts of personally identifiable information about millions of Americans. This information includes Social Security numbers, personal addresses, income and employment records, and tax return records. It is extremely important that CMS and the other federal agencies involved in the exchanges properly protect and maintain this sensitive information. However, yesterday's GAO report and the recent hacking of HealthCare.gov indicate that CMS is failing to perform this fundamental obligation.

GAO found that HealthCare.gov security weaknesses are due in part to CMS' failure to follow federal security standards for testing. The report indicates that CMS chose to do piecemeal testing of the website that suited CMS' needs, rather than the more rigorous testing that is federally mandated. The GAO report said, "Security control assessments for the FFM did not include tests of the full suite of security controls specified by [the National Institute of Standards

---

[1] Government Accountability Office. (2014, September). Healthcare.gov: Actions Needed to Address Weaknesses in Information Security and Privacy Controls. gao.gov

[2] *Wall Street Journal,* "Hacker Breached HealthCare.gov Insurance Site," Sept. 4, 2014.

and Technology] and CMS. The contractors that conducted these assessments reviewed only the security controls that CMS selected."[3]

GAO also found that CMS has yet to conduct a comprehensive security test of all the live components of the website working together in unison, sometimes referred to as end-to-end testing. When asked about comprehensive testing in your Questions for the Record after your November 5, 2013, congressional testimony, you wrote, "An independent security control assessor tested each piece of the FFM that went live on October 1 prior to that date."[4] GAO found that this testing is insufficient because testing each piece of the website separately means that the connections between the pieces go untested, thus allowing security vulnerabilities to go undetected. GAO's report recommends that CMS "perform a comprehensive security assessment of the FFM, including the infrastructure, platform and all deployed software elements."[5]

Furthermore, GAO found that CMS's Privacy Impact Assessment, required by the E-Government Act of 2002, did not assess the risks associated with the FFM's use of personally identifiable information.[6] CMS did not complete Computer Matching Agreements with the Peace Corps and the Office of Personnel Management, as required by the Computer Matching and Privacy Protection Act of 1988, for all federal agencies that exchange information.[7] CMS still has yet to document a security agreement governing third party interconnection with Equifax Workforce Solutions, which is responsible for verifying the income and employment status of exchange applicants.[8] Additionally, CMS lacked an alternate processing site to avoid major service disruptions, as recommended by the National Institute of Standards and Technology (NIST) Special Publication 800-34.[9]

As GAO has found in two previous reports,[10] mismanagement by CMS has impacted the quality of HealthCare.gov, in this case undermining the website's security. GAO's latest report states, "An important reason that all of these weaknesses occurred and some remain is that CMS did not and has not yet ensured a shared understanding of how security was implemented for the FFM

---

[3] Government Accountability Office. (2014, September). Healthcare.gov: Actions Needed to Address Weaknesses in Information Security and Privacy Controls. Page 48. gao.gov

[4] U.S. Senate Committee on Health, Education, Labor and Pensions Hearing: "The Online Federal Health Insurance Marketplace: Enrollment Challenges and the Path Forward." (2013, November 5). Marilyn Tavenner Questions for the Record.

[5] Government Accountability Office. (2014, September). Healthcare.gov: Actions Needed to Address Weaknesses in Information Security and Privacy Controls. Page 54. gao.gov

[6] *Ibid.* Page 44.

[7] *Ibid.* Page 45.

[8] *Ibid.* Page 43.

[9] *Ibid.* Page 49.

[10] Government Accountability Office. (2014, July). Healthcare.gov: Ineffective Planning and Oversight Practices Underscore the Need for Improved Contract Management. Page 11. gao.gov; Government Accountability Office. (2013, June). Patient Protection and Affordable Care Act: Status of CMS Efforts to Establish Federally Facilitated Health Insurance Exchanges. gao.gov

among all entities involved in its development."[11] For example, CMS identified one contractor as responsible for HealthCare.gov's firewalls. That responsibility was not listed in its statement of work, and that contractor indicated to GAO that it was another contractor's responsibility. CMS' announcement that HealthCare.gov was hacked this summer is a chilling reminder that these security weaknesses could have real consequences for everyday Americans. Even before the website went live on October 1, 2013, individuals within both CMS and the information technology (IT) community reported serious issues with HealthCare.gov's security. MITRE, the lead security testing contractor for the website, told CMS several times before the website was launched that it was vulnerable to hackers. Recognizing the serious nature of these concerns, CMS' Chief Information Security Officer recommended that the website should not be given an "Authority to Operate".[12]

CMS has assured the public that it has addressed all security concerns raised to date, but this recent hacking incident casts doubt on that claim. Additionally, CMS has numerous times attempted to prevent Congress from issuing copies of MITRE's security assessments, asserting that they could be used as a roadmap for hackers.[13] But if, as CMS has said, the website's security vulnerabilities have been addressed, it is unclear how hackers could exploit this information.

Additionally, CMS was not fully cooperative with GAO during its investigation. For example, GAO asked CMS for documentation regarding any security incidents with HealthCare.gov but was told that there had not been any incidents. Shortly thereafter, the CMS Chief Information Security Officer (CISO) testified in a congressional hearing that there had been 13 security incidents. When GAO again asked for the incident reports after the CISO's testimony, CMS did not provide them, and instead gave GAO a narrative description of the incidents. This description did not include enough information for GAO to determine the severity level of each incident.

The GAO concludes its report with a grim warning: "Until these weaknesses are fully addressed, increased and unnecessary risks remain of unauthorized access, disclosure or modification of the information collected and maintained by Healthcare.gov and related systems, and the disruption of service provided by the systems."[14] These continuing security issues surrounding HealthCare.gov are cause for concern not just by Congress but for all Americans who have a right to expect that the government will protect their information.

So that we may better evaluate the security of HealthCare.gov and CMS' actions to protect it, we ask that you provide answers to the following questions:

---

[11] Government Accountability Office. (2014, September). Healthcare.gov: Actions Needed to Address Weaknesses in Information Security and Privacy Controls. Highlights page. gao.gov

[12] Transcript, Interview of Teresa Fryer by the House Oversight and Government Reform Committee, Dec. 17, 2013, *available at* http://oversight.house.gov/wp-content/uploads/2013/12/Teresa-Fryer-ATO.pdf.

[13] *The Hill,* "Issa: Administration Lying about HealthCare.gov," Jan. 28, 2014. CMS also asked Senator Hatch and Senator Grassley not to release any MITRE documents, even in extremely redacted form, in its June 19, 2014 report, *Red Flags: How Politics and Poor Management Led to the Meltdown of HealthCare.gov.*

[14] Government Accountability Office. (2014, September). Healthcare.gov: Actions Needed to Address Weaknesses in Information Security and Privacy Controls. Highlights page. gao.gov

1. How many times has CMS identified attempts to compromise HealthCare.gov, and what was the outcome of those attempts? Please provide details about each incident including the date, the type of compromise attempted, the information implicated, and any actions CMS took to address or respond to the attack.

2. How many times has personally identifiable information processed by HealthCare.gov or the Data Hub been compromised? Please provide details about each incident including the date, how the information came to be compromised, and any actions CMS took to address or respond to the incident.

3. What actions has CMS taken to ensure personally identifiable information is protected?

4. To date, has CMS addressed all security issues identified by MITRE and any other security contractors? If no, why not?

5. Does HealthCare.gov fully comply with the Privacy Act of 1974 by protecting all individuals' personal information? To CMS's knowledge, has there ever been a time from October 1, 2013 to present when the website was not fully compliant with the Privacy Act of 1974?

6. To date, has CMS received any recommendations on the security of HealthCare.gov from sources including the Office of the Inspector General, the Office of Management and Budget, and the National Institute of Standards and Technology? If yes, please provide all recommendations and specify whether the recommendations have been implemented by CMS. Please provide a detailed explanation for any recommendations with which CMS did not concur, or that CMS has not yet implemented.

In addition, to provide greater assurances to the American people about the security of HealthCare.gov, we ask that you commit to the following actions:

1. Complete all of GAO's recommendations prior to the start of the next Open Enrollment Period on November 15, 2014, including:
    a. Conducting comprehensive security testing;
    b. Completing and documenting a Privacy Impact Assessment of HealthCare.gov, as required by the E-Government Act of 2002, that assesses the risks associated with the handling of personally identifiable information;
    c. Completing and documenting Computer Matching Agreements with the Peace Corps and the Office of Personnel Management, as required by the Computer Matching and Privacy Protection Act of 1988;
    d. Completing and documenting a security agreement governing third party interconnection with Equifax Workforce Solutions; and
    e. Developing an alternate processing site to avoid major service disruptions, as recommended by NIST Special Publication 800-34.

Thank you for your attention to this important matter. We would appreciate a response by no later than October 17, 2014.

Sincerely,

Senator Lamar Alexander
Ranking Member
Committee on Health, Education, Labor, and Pensions

Senator Orrin Hatch
Ranking Member
Committee on Finance

Senator Charles Grassley
Ranking Member
Committee on the Judiciary

Senator John Thune
Ranking Member
Committee on Commerce

Senator Rob Portman
Subcommittee Ranking Member
Committee on Homeland Security and Governmental Affairs

Congressman Fred Upton
Chairman
Committee on Energy and Commerce

Congressman Camp
Chairman
Committee on Ways and Means

Congressman Issa
Chairman
Committee on Oversight and Government Reform