

RON JOHNSON, WISCONSIN, CHAIRMAN

ROB PORTMAN, OHIO
RAND PAUL, KENTUCKY
JAMES LANKFORD, OKLAHOMA
MICHAEL B. ENZI, WYOMING
JOHN HOEVEN, NORTH DAKOTA
STEVE DAINES, MONTANA
JON KYL, ARIZONA

CLAIRE McCASKILL, MISSOURI
THOMAS R. CARPER, DELAWARE
HEIDI HEITKAMP, NORTH DAKOTA
GARY C. PETERS, MICHIGAN
MARGARET WOOD HASSAN, NEW HAMPSHIRE
KAMALA D. HARRIS, CALIFORNIA
DOUG JONES, ALABAMA

United States Senate

COMMITTEE ON
HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

WASHINGTON, DC 20510-6250

October 20, 2018

The Honorable Alex Azar II
Secretary
U.S. Department of Health & Human Services
200 Independence Avenue, S.W.
Washington, D.C. 20201

Dear Secretary Azar:

On Friday, October 19, 2018, the Centers for Medicare & Medicaid Services (CMS) notified the Committee of a breach of a system associated with healthcare.gov, the website created for Obamacare enrollment. According to CMS, the breach affected approximately 75,000 individuals through the Direct Enrollment pathway for agents and brokers of the Federally-facilitated Exchange.¹ This breach follows CMS's history of reported security weaknesses with the healthcare.gov web portal and supporting systems.² Previous congressional oversight showed how CMS launched healthcare.gov in 2013 despite vulnerabilities that put the personal information of Obamacare enrollees at risk.³

The Committee has jurisdiction over federal information systems and the Federal Information Security Management Act of 2002 (FISMA).⁴ To assist the Committee in its oversight of the breach affecting healthcare.gov, I respectfully request the following information:

¹ Letter from Seema Verma, Administrator of Centers for Medicare & Medicaid Services, U.S. Department of Health & Human Services, to Chairman Ron Johnson and Ranking Member Claire McCaskill, Senate Committee on Homeland Security & Governmental Affairs (Oct. 19, 2018) (on file with Committee staff).

² U.S. Government Accountability Office, GAO-16-265, *Healthcare.gov: Actions Needed to Enhance Information Security and Privacy Controls* (Mar. 23, 2016), <https://www.gao.gov/mobile/products/GAO-16-265> (finding, "However, GAO identified weaknesses in technical controls protecting the data flowing through the [Federal Data Services Hub]. These included insufficiently restricted administrator privileges for data hub systems, inconsistent application of security patches, and insecure configuration of an administrative network. GAO also identified additional weaknesses in technical controls that could place sensitive information at risk of unauthorized disclosure, modification, or loss. In a separate report, with limited distribution, GAO recommended 27 actions to mitigate the identified weaknesses.").

³ See, *Fact Sheet: Healthcare.gov Launch: Security Vulnerabilities and Lack of Testing Put Personal Information of Site Users at Risk*, U.S. House Committee on Oversight & Government Reform (Jan. 7, 2014), <https://oversight.house.gov/release/fact-sheet-healthcare-gov-launch-security-vulnerabilities-lack-testing-put-personal-information-site-users-risk>; see also, Jessica Meyers, *Security Experts Fear ACA Vulnerabilities*, Politico (Nov. 6, 2013), https://www.politico.com/story/2013/11/security-experts-fear-obamacare-affordable-care-act-data-protection-problems-99430_Page2.html.

⁴ See, Senate Rule XXV(k); S. Res. 445 (108th Cong.); S. Res. 62 (115th Cong.).

1. Please provide the date and time by which the first indicator of compromise (IOC) was identified and who identified this initial IOC (i.e., CMS personnel or contractors, or law enforcement entities).
2. Please provide the date on which CMS notified the Office of Inspector General and law enforcement.
3. Please describe the type of personally identifiable information (PII) affected, and how CMS determined that the 75,000 was the universe of individuals affected. Does CMS believe this to be the full exposure, or is 75,000 CMS's initial estimate?
4. Please provide a copy of CMS's notification to U.S. Computer Emergency Readiness Team concerning the initial IOC.
5. Please provide the date on which the bad actor(s) were expunged from the system; log information sufficient to indicate how long these bad actor(s) had access to CMS or HHS system(s) and also individuals' PII; and CMS's current assessment as to whether all bad actor(s) have been expunged from CMS and HHS systems.
6. Has CMS notified the 75,000 people who have had their sensitive information compromised? Does CMS intend to offer any credit monitoring or protection to these individuals?
7. Please produce all documents or communications referring or relating to the breach of healthcare.gov's Direct Enrollment pathway.

In addition to responses to the above, I respectfully request a briefing for Committee staff. Please provide a response as soon as possible but no later than 5:00 p.m. on October 30, 2018.

The Committee on Homeland Security and Governmental Affairs is authorized by Rule XXV of the Standing Rules of the Senate to investigate "the efficiency, economy, and effectiveness of all agencies and departments of the Government."⁵ Additionally, S. Res. 62 (115th Congress) authorizes the Committee to examine "the efficiency and economy of operations of all branches and functions of Government with particular references to (i) the effectiveness of present national security methods, staffing, and processes...."⁶

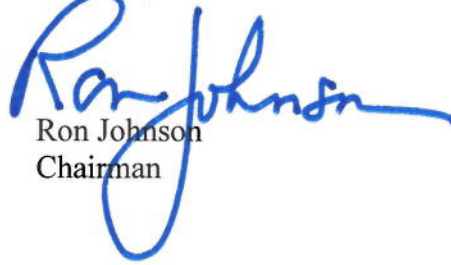
If you have any questions about this request, please ask your staff to contact Elliott Walden of the Committee staff at (202) 224-4751. Thank you for your attention to this matter.

⁵ S. Rule XXV(k); see also S. Res. 445, 108th Cong. (2004).

⁶ S. Res. 62 § 12, 115th Cong. (2017).

The Honorable Alex Azar II
October 20, 2018
Page 3

Sincerely,



Ron Johnson
Chairman

cc: The Honorable Claire McCaskill
Ranking Member

Ed Simcox
Acting Chief Information Officer
U.S. Department of Health & Human Services