

DIANE BLACK
6TH DISTRICT OF TENNESSEE

COMMITTEE ON
WAYS AND MEANS

SUBCOMMITTEE ON HEALTH

COMMITTEE ON THE BUDGET



CONGRESS OF THE UNITED STATES
HOUSE OF REPRESENTATIVES
WASHINGTON, DC 20515

DISTRICT OFFICES

355 NORTH BELVEDERE DRIVE
SUITE 308
GALLATIN, TN 37066
(615) 206-8204
(615) 206-8980 (FAX)

321 EAST SPRING STREET
SUITE 301
COOKEVILLE, TN 38501
(931) 854-0069

July 9, 2015

The Honorable Sylvia Matthews Burwell
Secretary
U.S. Department of Health and Human Services
200 Independence Avenue, SW
Washington, DC 20201

The Honorable Andy Slavitt
Acting Administrator
Centers for Medicare and Medicaid Services
200 Independence Avenue, SW
Washington, DC 20201

Dear Secretary Burwell and Acting Administrator Slavitt:

Over the past year, America has witnessed a disturbing trend of security breaches involving government-run websites, including those run by the Internal Revenue Service (IRS) and the Department of Health and Human Services (HHS). On July 8, 2014, the Committee on Science, Space, and Technology held a hearing concerning the Office of Personnel Management (OPM) security breach, which constituted one of the largest government data breaches in history. At this hearing, Gregory Wilshusen, the Director of Information Security Issues at GAO testified that the Office has repeatedly found weaknesses in government information technology (IT) controls and systems but recommendations for action to improve these systems have largely not be followed.

Of particular concern is Mr. Wilshusen's testimony that the number of security incidents involving personally identifiable information (PII) being compromised has more than doubled since 2009, including social security numbers and addresses.¹ HealthCare.gov and its connected systems now house some of the largest receptacles of American's PII. In September 2014, the Government Accountability Office (GAO) issued a report entitled "HealthCare.gov: Actions Needed to Address Weaknesses in Information Security and Privacy Controls," which outlined the remaining weaknesses in information security and privacy and the residual flaws in the technical implementation of security controls.² At the July 8th hearing, Mr. Wilshusen testified that the recommended risk assessments for HealthCare.gov had yet to be completed by HHS despite these being required by the Office of Management and Budget and recommended by GAO nearly a year ago. According to Mr. Wilshusen's testimony, such assessments remain "vitally important" to developing the security of the site.

Similarly, the Multidimensional Insurance Data Analytics System (MIDAS) was also launched without a privacy risk assessment. The MIDAS system is an enormous data warehouse that retains PII of

¹ U.S. Government Accountability Office. (2015). *Information Security- Cyber Threats and Data Breaches Illustrate Need for Stronger Controls Across Federal Agencies*. ONLINE. GPO Access. 8 July 2015. Available: <http://science.house.gov/sites/republicans.science.house.gov/> [9 July 2015].

² U.S. Government Accountability Office. (2015). *Healthcare.gov- Actions Needed to Address Weaknesses in Information Security and Privacy Controls*. ONLINE. GPO Access. Sept 2014. Available: <http://www.gao.gov/assets/670/665879.pdf> [9 July 2015].

individuals who opened accounts on HealthCare.gov even if they did not enroll in coverage. Information retained in MIDAS includes names, Social Security numbers, birthdates, addresses, phone numbers, passport numbers, employment status, and financial accounts. According to reports, this information is stored by the system indefinitely.³ Similarly, the GAO report from September 2014 stated that without such risk assessments, “It will be difficult for CMS to demonstrate that it has . . . taken steps to ensure that the privacy of that data is protected.”

In addition to concerns over privacy risk assessments, numerous security issues surrounding HealthCare.gov and its related systems remain. It is clear that HHS and other agencies that handle and store PII are ignoring repeated warnings and recommendations. The GAO has definitively stated that “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.” It is equally disturbing that there is still no requirement for the Administration to notify users if and when their PII is compromised on the federal exchange and its related systems. I remain extremely concerned about the risks associated with HealthCare.gov and the PII of millions of Americans.

Americans should not be put at risk because of the Administration’s inability to construct a secure website and respond to repeated warnings from both the GAO and Congress. To this end, I request a thorough update on the status of implementing each of the recommendations enclosed in the September 2014 GAO report on HealthCare.gov’s data security. Additionally, please detail any oversight plans to ensure that the recommendations are being executed in a timely and thorough manner.

I respectfully ask that you provide this information by July 23, 2015. Should you have any questions, please contact Katie Allen at Katie.Allen@mail.house.gov in my office.

Sincerely,



Diane Black
Member of Congress

³ Alonso-Zaldivar, R. (2015, June 15). Vast data warehouse raises HealthCare.gov privacy concerns. *Yahoo: Associated Press*. Retrieved from <http://news.yahoo.com/vast-data-warehouse-raises-health-overhaul-privacy-concerns-072607026.html>