

**Congress of the United States**  
**Washington, DC 20515**

October 15, 2013

Mr. Daniel R. Levinson  
Inspector General, U.S. Department of Health and Human Services  
330 Independence Ave, SW  
Washington, D.C. 20201

Dear Inspector General Levinson:

It is widely understood that every information system can be hacked. Cybersecurity is now one of the greatest threats our nation faces. Bad actors are constantly attacking our information infrastructure and looking for opportunities to expose vulnerabilities. Rapidly evolving technology presents a never-ending challenge to safe-guard against catastrophic attacks. Given these realities, we are concerned for the integrity and security of the Data Services Hub (Data Hub)—the new launching pad for the names, addresses, social security numbers, and residency status of Americans seeking health insurance on the federal exchanges.

Systems of this complexity require sufficient time to ensure the fundamental and necessary controls that protect data systems are met. Specifically, prior to launching a new data system where consumers will provide their most sensitive personal information, a series of front-end controls should be put in place. However, it is unclear if certain critical best practices were conducted prior to releasing the Data Hub—such as pilot programs and employing White Knight hackers to provide feedback on the system’s vulnerabilities. Furthermore, reports that your office did not review the draft and final security designs for the Data Hub is concerning.

Taking all these factors into account, it is imperative that Congress be provided with the information necessary to understand how the Data Hub was certified and what continuing controls have been put in place to protect Americans who are currently accessing the system. Specifically, we request information on the user access controls for the Department of Health and Human Services (HHS) staff and Navigators that have been determined appropriate for using the Data Hub. Additionally, what system has been implemented to monitor the behavioral patterns of the system to identify suspicious activity?

With regard to the Navigator Program, which does not require a background check for the individuals who will interface directly with the public, what measures have been put in place to ensure accountability? What checks and balances have been put in place to protect Navigators from claims of fraud and abuse? Has HHS implemented continuing education programs necessary to ensure Navigators are aware of the most up-to-date fraud and cybersecurity threats?

Cybersecurity threats also exist as users log into the system, input their personal information, and remain on the internet. What controls are in place to protect Americans from these “man-in-the-middle” attacks?

As you are aware, HHS completed its Final Security Control Assessment (SCA) and issued a Security Authorization Decision. Following this action, on October 1, 2013, the Data Hub was fully implemented. We respectfully request your office provide us with a copy of the Final SCA report, including but not limited to the Certification and Accreditation (C&A) plan, in addition to the Interim Authority To Operate (IATO) or the Authority to Operate (ATO).

If an IATO was issued, we request a copy of this decision, as this report would indicate all known vulnerabilities that were identified, in addition with the current plan to ensure corrective action. If an ATO was issued, we seek to understand who defined the controls that the system must adhere to, as directed by the Office of Management and Budget (OMB), in addition to information detailing whether or not the controls were met, or were deemed deficient. Finally, we request a copy of the mitigation plan that the U.S. Chief Information Officer approved that certifies the Data Hub may be fully implemented.

HHS and the Centers for Medicare and Medicaid Services (CMS) have filed their action, "Notice to establish a new system of records" for the Data Hub in the Federal Register. This action reads, "records are maintained with identifiers for all transactions for a period of 10 years after they are entered into the system" (FR Doc No: 2013-02666). At a House Committee on Oversight and Government Reform hearing on July 17, 2013, Congress was informed by CMS that records obtained from the Data Hub would not be maintained. This statement is in direct conflict with the Federal Register. We ask that you provide further clarification on the authority by which HHS may receive records and not maintain the data.

Thank you in advance for your attention to this letter. We look forward to your prompt reply.

Sincerely,



Diane Black  
Member of Congress



Patrick Meehan  
Member of Congress

cc:

Mr. Steven VanRoekel  
U.S. Chief Information Officer, Office of Management & Budget  
1650 Pennsylvania Avenue, NW  
Eisenhower Executive Office Building, Room 262  
Washington, DC 20503

Mr. Kevin Charest  
Chief Information Security Officer, Department Health and Human Services  
200 Independence Ave SW  
Washington, D.C., DC 20201