



DEPARTMENT OF HEALTH & HUMAN SERVICES

Office of the Assistant Secretary
for Legislation

Washington, D.C. 20201

December 13, 2013

The Honorable Darrell Issa
Chairman
Committee on Oversight and Government Reform
U.S. House of Representatives
Washington, D.C. 20515

Dear Mr. Chairman:

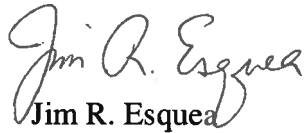
Earlier today, we reached out to your staff to request a meeting so that a group of cybersecurity experts could explain our concerns regarding the sensitive security testing documents for HealthCare.gov that you have subpoenaed from the MITRE Corporation (MITRE). We are disappointed that you have not taken us up on our offer to discuss with you ways to protect the highly sensitive information contained in these documents from determined actors seeking to compromise the security and functioning of the website. As you know, we have been trying to engage in a productive dialogue with you on these issues for almost two weeks – in letters sent on December 4th, December 9th, and December 12th.

To be clear, HealthCare.gov and the related Federal IT systems are compliant with the Federal Information Security Management Act (FISMA), based on standards promulgated by the National Institutes of Standards and Technology (NIST) and there is a robust process of ongoing security assessments to identify and remediate security risks. As we described in detail during a Congressional briefing for Members, there have been no successful security attacks on HealthCare.gov and no person or group has maliciously accessed personally identifiable information from the site. Our concern is not the current security status of the website, but the threat to the security of the site created by releasing documents that could provide a roadmap for malicious cyber actors to direct more efficient and effective cyber-attacks against some of the most sensitive sites the Federal government operates.

It is important that these cybersecurity concerns are not held by the Department of Health and Human Services alone. The meeting we proposed earlier today would have included a senior cybersecurity official from the Department of Homeland Security, and the United States Chief Information Officer, who were prepared to explain the harmful impact that disclosure of these security documents could have in allowing hackers to penetrate not only HealthCare.gov and the Federal Data Services Hub, but other Federal IT systems, some of which contain taxpayer information. I understand that the Internal Revenue Service shares these concerns and is prepared – along with the agencies cited above – to discuss them with you. Moreover, I understand that these same concerns have been raised repeatedly by MITRE in response to your subpoena for unredacted copies of the documents.

We remain anxious to discuss a protocol for the handling of sensitive security documents that would satisfy legitimate oversight interests while addressing our security concerns, and will be available at your convenience.

Sincerely,

A handwritten signature in black ink, appearing to read "Jim R. Esquea". The signature is fluid and cursive, with the first letters of the first and last names being capitalized and prominent.

Jim R. Esquea
Assistant Secretary for Legislation

cc: The Honorable Elijah Cummings
Ranking Member