Congress of the United States
Washington, DC 20515

April 17, 2014

The Honorable Kathleen Sebelius Secretary U.S. Department of Health and Human Services	The Honorable Jacob Lew Secretary U.S. Department of the Treasury
The Honorable Jeh Johnson Secretary U.S. Department of Homeland Security	The Honorable John Koskinen Commissioner U.S. Internal Revenue Service

Dear Secretary Sebelius, Secretary Lew, Secretary Johnson, and Commissioner Koskinen:

We are writing to you because your agencies have a stake in the healthcare.gov website, and we are concerned about its security. We believe that malicious actors have the potential to violate the privacy of Americans who attempt to comply with the individual mandate and purchase a health insurance plan over the website.

Healthcare.gov represents a particularly attractive target for bad actors since it is the gateway to a virtual treasure trove of private personal data. As of March 11, the Department of Health and Human Services (HHS) reported that 2.6 million Americans have selected a marketplace plan over the healthcare.gov website. This means that these individuals have submitted information including birthdates, social security numbers, income, work history and health status to healthcare.gov.

We want to protect the privacy of Americans, and in the spirit of this common goal we feel compelled to bring a specific and widespread cyber threat to your immediate and personal attention, and suggest an existing solution that can be executed quickly and without great expense. Specifically, a digest of known bad, exploitable components present in the current site can be created quickly. Those who have a unique purview over the open source Central Repository know that CGI, which was until recently the primary vendor at healthcare.gov, uses highly exploitable versions of Apache Struts; which, if present in healthcare.gov, should be removed immediately and updated with the existing non-exploitable versions. Because HHS recently dismissed CGI as the primary vendor for the website, we feel that this issue is especially timely, as its successor may have to deal with these problems.

Today's software leverages open source software that takes the form of pre-fab building blocks, or components, that fit together to form the basis of a website. Approximately 90% of any piece of software is made up of these open source components and only ten percent of software is custom written code. While software development is enormously more efficient today, these common building blocks are also becoming much more attractive targets for cyber exploit. This means that websites are becoming increasingly vulnerable to breaches.

A primary reason these vulnerabilities are becoming so widespread is that existing Federal regulations for validating code do not address the use of these open source components, because they are not considered to be code. These regulations were written prior to the practice of software assembly and the widespread proliferation of open source. This is a growing problem, as more than 13 billion components were downloaded from the open source community in 2013 alone.

Federal integrators, including those involved with Healthcare.gov, download thousands of unique components every month, a substantial portion of which have exploitable security defects. In fact, recent studies show that more than 75% of all software applications have open source components that contain severe known and identifiable security defects, as classified by the National Institute of Standards and Technology.

We request that you institute an agency-wide effort to review your use of open source components, identify all vulnerable open source components in your applications, and replace those components. Thank you for your time and attention regarding this issue. We eagerly await your response.

Sincerely,

Lynn Jenkins
Lynn Jenkins, CPA

Diane Black
Diane Black

Dan Benishek
Dan Benishek

Kerry Bentivolio
Kerry Bentivolio

Tom Marino
Tom Marino

Stephen Fincher

Michael Conaway

Bill Cassidy
Bill Cassidy