Rep. Joseph R. Pitts
Opening Statement
Energy and Commerce Subcommittee on Health Hearing:
"Examining Cybersecurity Responsibilities at HHS"
Wednesday, May 25, 2016 (10:00 AM)

The Subcommittee will come to order.

The Chairman will recognize himself for an opening statement.

In today's digital, connected world, cybersecurity is one of the most important, most urgent problems that we as a society face. Indeed, a great deal of sensitive information has been entrusted to the federal government, and as the recent breach at the Office of Personnel Management showed, we are not always the most sophisticated at protecting that information. We therefore must always be on the look-out for opportunities to improve and adapt to changing cybersecurity threats and realities.

As a result of an investigation conducted by the Energy and Commerce Subcommittee on Oversight and Investigations to examine information security at the U.S. Food and Drug Administration, it was determined that serious weaknesses existed in the overall information security programs at the U.S. Department of Health and Human Services (HHS). It seems a major part of the problem is the organizational structure in place at HHS that puts information security second to information operations.

This stems from the fact that, right now, the top official responsible for information operations at HHS is the Chief Information Officer, or CIO, and the official responsible for information security, the Chief Information Security Officer, or CISO [CIZ-O] reports to him. In other words, the official in charge of building complex information technology systems is *also* the official in charge of ultimately declaring those systems secure. This is an obvious conflict of interest.

Today's hearing will take a closer look at bipartisan legislation designed to address these organizational issues. H.R. 5068, recently introduced by our Energy and Commerce Committee colleagues, Reps. Long and Matsui, is known as the HHS Data Protection Act. This bipartisan bill elevates and empowers the current HHS

CISO with the creation of the Office of the Chief Information Security Officer within the Department of Health and Human Services, which will be an organizational peer to the current Office of the Chief Information Officer.

This type of structure is not novel or untested: a branch of the Department of Defense has already implemented a similar structure, and many industry experts such as PricewaterhouseCoopers now recommend that CIOs and CISOs be separated "to better allow for internal checks and balances."

We are very lucky today to have expert witnesses who can talk to us about not only the bill itself, but help us understand more about the CIO-CISO relationship and why the structure currently in place at HHS could benefit from an update. In particular, I'd like to highlight that one of our witnesses, Mr. Mac McMillan, experienced the very structure that H.R. 5068 seeks to create at HHS during his time working for the Department of Defense, and will be able to provide valuable perspective on how HHS might implement this reform.

Today's hearing provides Members an important opportunity to examine cybersecurity responsibilities at HHS, and to discuss a bill that will help raise the visibility and priority of information security across the Department.