Opening Statement of Chairman Fred Upton
Subcommittee on Health Hearing "Examining Cybersecurity Responsibilities at HHS"
May 25, 2016

The House Energy and Commerce committee knows, better than I think just about any committee on the Hill, how important cybersecurity is. We've examined issues surrounding encryption, considered how best to address data breaches, and even dug deep into the protocols that run our cell phones, studying the vulnerabilities. We understand that our digital infrastructure is under attack – every second of every day – from actors of all motivations and levels of sophistication.

And that is why we are here today. Just like every other federal department and private organization, HHS's networks and the information contained within them are under constant threat. At first glance, some may assume that we're holding today's hearing to chastise HHS for cybersecurity incidents that have happened in the past. We are not.

We are holding this hearing because we are looking to the future. We are holding this hearing to examine whether or not HHS has the opportunity, by embracing the reforms suggested in Mr. Long's and Ms. Matsui's bipartisan bill, not only to improve its own internal cybersecurity, but to become a leader in cybersecurity within the federal government and in the health care industry.

Consider this: the current structure for cybersecurity officials in place at HHS was originally mandated in 2003. The Internet looked radically different 13 years ago; smartphones were rare, cloud computing had yet to really take off, and the biggest

threats to our digital infrastructure were viruses and worms, both of which could be stopped using standard firewalls and anti-virus software.

But the cyber world is constantly changing, and the threats that we faced 10 years ago are not the threats that we face today. Instead, we face a daunting array of cybersecurity threats, from sophisticated thefts of personal information held by health care providers, to the hostage-taking of hospital networks and equipment by ransomware.

So I hope Members will take this opportunity to examine closely the issue before us, and give careful consideration as to whether or not an organizational structure established a decade ago is as agile, versatile, and powerful as we need it to be in order to combat the growing threats that we face.

Our oversight identified a problem. And we have a thoughtful solution in the HHS Data Protection Act to address it.