Opening Statement of Chairman Greg Walden
Subcommittee on Oversight and Investigations
Hearing on "Examining the Role of the Department of Health and Human Services in Health Care Cybersecurity"
June 8, 2017

Our lives continue to become more interconnected every day. This explosion of digital connectivity and information technology provides us with previously unimaginable convenience, engagement, capabilities, and opportunities for innovation.

For all its benefits, however, the digitization of our daily lives also comes with risk. The internet and information technologies are inherently insecure. With time, motivation, and resources, someone halfway around the world can find a way into almost any product system.

As the opportunities for attackers proliferate, the potential consequences of their actions are becoming more severe. As more products, services, and industries become connected to the digital world, we must acknowledge that the threat is no longer just data and information – it is public health and safety.

For the health care sector, these factors present a very real threat – and equally daunting challenge. As we witnessed with the recent WannaCry ransomware outbreak, portions of the National Health System in the U.K. had to turn away patients except for emergency care after vulnerable systems fell victim to the exploit.

WannaCry did not appear to be a targeted attack on health care, but the potential consequence of the exploit on health care – including patient safety – was far more severe. If this had been a more sophisticated exploit, or a targeted attack on the health care sector, the consequences could have been far worse.

The health care sector is starting to grasp this new reality but, as noted in the recent task force report, which we will discuss today, health care cybersecurity is in "critical condition" and requires "immediate and aggressive attention."

Which brings us to today's hearing. Clearly, the sector needs leadership. HHS is uniquely situated to fill this void. Historically, the Department has struggled to effectively embrace this responsibility, but that trend cannot continue.

More recently, HHS has started to demonstrate a commitment and focus to addressing the rampant challenges in health care cybersecurity. For example, the Department's actions in response to the WannaCry ransomware - coordinated through the newly established HCCIC - have generally received praise from the sector.

This and other recent actions are positive signs that the Department is heading in the right direction. But HHS has a long way to go to demonstrate the leadership necessary to inspire change across the sector. It needs to be open and transparent about who is in charge and provide clarity about the roles and responsibilities, not only internally but across the sector. They need to make sure that a small rural hospital not only knows exactly who to call, but also has access to the resources and information to keep their patients safe.

This hearing provides an opportunity for HHS to provide some much needed clarity about its internal structure, as well as outline its plan to elevate cybersecurity across the sector.

The sector is operating on borrowed time. The cyber threat is spreading and, left unchecked, it will pose an increasingly greater threat to public health.