Opening Statement of Chairman Greg Walden
Subcommittee on Oversight and Investigations
Hearing on "Cybersecurity in the Health Care Sector: Strengthening Public-Private Partnerships"
April 4, 2017

(As prepared for delivery)

We are well aware of the threats posed by our increasingly connected society, but nowhere do these risks hit closer to home than on the very technology we rely on for our own health care. The threats range from ransomware, breaches of patient data at heath care organizations, to the vulnerabilities in pacemakers and other medical devices. Taken in isolation, these and other threats pose serious challenges to health care organizations. Collectively, they demonstrate the breadth, complexity, and unavoidable nature of cyber threats in modern society – both now and for the foreseeable future.

As technology becomes increasingly integrated with all levels of our health care, cyber threats pose a challenge to the entire sector. Everyone - from the smallest rural hospitals, to large providers and device manufacturers - faces some level of exposure and risk.

Breaches, exploits, and vulnerabilities are inevitable realities of modern society, even for the most well-resourced and sophisticated organizations. But this does not mean doom-and-gloom for everyone with an internet connection. It is simply reality and must serve as the baseline for any discussion about cybersecurity. We may not be able to stop every attack, but as the threats continue to escalate, we must do more to minimize the risk.

Improving security is a collective responsibility. When we work together – government and private sector, large companies and small – we can do more to improve security than if we attempt to solve it on our own.

An attack on one organization may be prevented elsewhere if we have the infrastructure and mechanisms necessary to communicate effectively with others across the sector. Further, if an event has widespread or national implications, we need to coordinate an effective and efficient response – with unity of effort, not confusion over roles and responsibilities.

That is why, for almost two decades, the U.S. has worked to establish public-private partnerships to coordinate security planning and information sharing within and across our 16 critical infrastructure sectors, which includes health care.

Effective collaboration between government and the private sector is vital to elevating our security posture,. These partnerships provide a vital link between those responsible for the safety and security of the nation with those who own and operate the infrastructure critical to those objectives.

To date, these public private partnerships have experienced mixed results. Some sectors have been more successful than others in coming together – both with private sector and government partners. The health care sector, in particular, has struggled to coalesce around these public-private partnerships for cybersecurity. It is this shared, goal that brings us together today.

This hearing marks an important opportunity to hear from our distinguished panelists about what is necessary to bring the health care sector together and continue building momentum in the right direction. Simply put, the cost of inaction is too great. As the threats continue to escalate, so too do our cybersecurity challenges. We've seen the headlines – we know the attacks will continue. But today is about what improvements can be made so we can be prepared for the inevitable.