Opening Statement of The Honorable Tim Murphy
Subcommittee on Oversight and Investigations
Hearing on “Cybersecurity in the Health Care Sector: Strengthening Public-Private Partnerships”
April 4, 2017

We are here today to talk about cybersecurity in the health care sector. Strong cybersecurity practices are essential in this industry. This isn’t just about protecting patient data or information – this is about patient safety.

For nearly two decades, a cornerstone of the nation’s efforts to combat cyber threats have been public-private partnerships designed to facilitate engagement and collaboration between the government and private sector. Over time this model has evolved, but the objective remains the same – unity of effort between those responsible for protecting the nation and those who own and operate the infrastructure that is critical to that mission.

The focal point of these efforts are 16 critical infrastructure sectors—one of which is the health care sector. Each sector is organized around several key institutions – a Sector Specific Agency, Government Coordinating Council, Sector Coordinating Council and Information Sharing and Analysis Center. Each of these institutions plays an important role in ensuring participation, collaboration, and unity of effort of the government and private sector participants within each sector.

Despite a number of efforts to improve this model over the years, it has achieved mixed results across the various sectors. Some sectors have succeeded in developing robust support and engagement with both government and industry participants.

The gold standard, to date, has been the financial sector. This sector enjoys a strong, collaborative relationship with their government partner – the Department of the Treasury – which is noteworthy because Treasury is also their regulator. In addition, despite having a very diverse sector, they have succeeded in encouraging support and participation from a wide variety of institutions – from small community banks to large multi-national financial institutions. This extensive membership has helped the sector to establish the nation’s most sophisticated and well-resourced ISAC, which improves its value to the entire sector.

Another, more recent, success story has been the electricity sector. This sector has improved collaboration and engagement – both with government partners at the Department of Energy and across private industry – through senior executive participation on the sector coordinating council. In addition to elevating the priority for industry partners, it has improved coordination and unity of effort with the government.

Despite the relative success of these and several others, every sector has unique characteristics and challenges that influence the pace of adoption and engagement in these institutions. What works for one sector may not work for others. As each sector figures out what works best for their participants, however, the lessons from others should not be overlooked or ignored – especially for those sectors that continue to evolve.

Which brings us to the focus of today's hearing – the health care sector. This sector has long struggled to coalesce around the public-private partnership model, especially with respect to cybersecurity. This may be partially attributable to the fact that cybersecurity is a relatively new challenge for much of this sector. However, as health care becomes increasingly digitized, the need to improve cybersecurity must be a priority.

Gaining the acceptance and support necessary to overcome historical obstacles will not be easy for this sector. To start, health care is an incredibly diverse and complex sector, with a wide range of industries and institutions of varying sizes, technological sophistication, and resources. It is also a sector where cybersecurity often becomes conflated with privacy or compliance, complicating the discussion. This, in turn, is exacerbated by the fact that a successful public-private partnership depends on collaboration and trust with HHS – an understandable challenge given the many participants in the sector who are regulated by various entities within the Department.

These and other challenges are understandable and daunting. If I am a small, rural health care institution – where cybersecurity falls to one employee who is also responsible for managing IT systems and fixing copiers, among other duties – what value do I get for the cost of joining the ISAC or listening to guidance from the sector coordinating council? At present, it is hard to answer that question, especially for those institutions already operating on negative margins.

These challenges, however, must be overcome. The cost of failure – for patients, as well as health care institutions – is too great. Cybersecurity incidents can result in life or death situations if a medical device is hacked, or an attack shuts down a hospital's computer systems. Cybersecurity is a collective responsibility and that is why it is imperative that this sector find a way to come together to find a sustainable path forward.

I look forward to hearing more from our witnesses about the challenges of this sector and what is needed to bring unity and commitment from all participants. These are the folks working in the trenches and while the sector has shown signs of progress, much work remains to be done.