Opening Statement of The Honorable Tim Murphy
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

(As prepared for delivery)

We are here today to continue our examination of cybersecurity in the health care sector. As we discussed at our hearing in April about the role of public-private partnerships, cybersecurity in this sector ultimately comes down to patient safety. And we got a glimpse just weeks ago at what a large-scale cyber incident could do to the health care sector—including the impact on patients—during the WannaCry ransomware event. Today, we turn to the role of the Department of Health and Human Services (HHS) in health care cybersecurity.

Recognizing the critical importance of cybersecurity in this sector, two years ago, in the Cybersecurity Act of 2015, Congress asked HHS to undertake two evaluations—one evaluating the Department's internal preparedness for managing cyber threats, and a second done alongside industry stakeholders examining the challenges of cybersecurity in the health care sector. These evaluations are now complete, and give not only the Congress, but the entire health care sector, an opportunity to better understand the agency's approach to cybersecurity. The reports also allow us to establish a baseline for evaluating HHS' progress moving forward.

HHS's internal preparedness report sets out the roles and responsibilities of various HHS offices in managing cyber threats, among other information. For example, the report identified a single HHS official – the cybersecurity "designee" – as having primary responsibility for cybersecurity efforts across the agency. But what precisely does this mean, and how does this cybersecurity designee work with the eleven components identified by HHS as having cybersecurity responsibilities? In addition, the Committee has learned that many of the details may already be obsolete due to recent and ongoing changes in HHS's internal structure.

For example, HHS's creation of a Health Cybersecurity and Communications Integration Center (HCCIC), modeled on the National Cybersecurity and Communications Integration Center (NCCIC) operated by the Department of Homeland Security, could dramatically change how HHS handles cyber threats

internally. It is our understanding that the HCCIC will serve as a focal point for cyber threat information collection and dissemination from HHS's internal networks, as well as external sources. However, details about this new function remain limited. Therefore, how the HCCIC fits in to the Department's internal structure and preparedness, as well as its role with respect to private sector partners will be a focus of today's discussion.

The second report, released late last week, focuses broadly on the challenges of cybersecurity in the health care industry. This report reflects the findings and recommendations of the Health Care Industry Cybersecurity Task Force. The Task Force members were selected from a wide-range of stakeholders, including federal agencies, the health care sector and cybersecurity experts. The report does not mince words, broadly concluding that health care cybersecurity is in critical condition. The report identified six imperatives—such as defining leadership and expectations for the industry, increasing the security of medical devices and health IT, and improving information sharing within the industry—and made 27 specific recommendations. Many of these recommendations call on HHS to provide more leadership and guidance for the sector as a whole.

It is clear from these reports that there is much that HHS can and should do to help elevate cybersecurity across the sector. The importance of meeting this challenge head-on was illuminated in recent weeks by the widely-publicized WannaCry ransomware. Frankly, we are lucky that that United States was largely spared from this infection, which temporarily crippled the National Health Service in England. Doctors and nurses were locked out of patient records. Hospitals diverted ambulances to nearby hospitals and cancelled non-emergency services after widespread infection of the ransomware.

This incident was an important test of HHS's response to a potentially serious event and thus far, the feedback has been positive. Reports suggest that HHS took a central role in coordinating resources, disseminating information and serving as a nerve center for public-private response efforts. But this was just one incident, and HHS must remain vigilant. The WannaCry infection was not the first widespread cyber incident, nor will it be the last.

Therefore, a commitment to raising the bar, for all participants in the sector – no matter how large or small, needs to be embraced. This is a collective responsibility and HHS has an opportunity to show leadership and to set the tone. Because this is no longer just about protecting personal information or patient data. This is about patient safety.

I want to thank our witnesses for appearing today and look forward to learning more about HHS's efforts on this important topic. I now recognize the Ranking Member, Ms. DeGette, for her opening statement.