COMMITTEE ON
ENERGY & COMMERCE
DEMOCRATS
RANKING MEMBER FRANK PALLONE, JR.
NEWS

FOR IMMEDIATE RELEASE
June 8, 2017

CONTACT
CJ Young — (202) 225-5735

Pallone: We Need to Up Our Game Against Cyberattacks

"We must make sure that HHS has the resources it needs to develop and implement a robust cybersecurity strategy"

Washington, D.C. – *Energy and Commerce Ranking Member Frank Pallone, Jr. (D-NJ) delivered the following opening remarks at an Oversight and Investigations Subcommittee hearing titled, "Examining the Role of the Department of Health and Human Services in Health Care Cybersecurity:"*

Mr. Chairman, thank you for holding this hearing today.

This Committee has a long history of examining cybersecurity. The federal government continues to make progress toward addressing vulnerabilities in the health care sector, but it is clear that we still have a lot of work to do.

For example, the 2015 Anthem attack highlighted the need for all industry members to come together and find solutions to cyber threats. More recently, the "WannaCry" ransomware attack demonstrated that cyberattacks have real world consequences that can place patients at risk.

And now, with the interconnection of health records – and a network of connected medical devices – the threat of cyberattacks on critical parts of our health care infrastructure is ever-present.

While there is no single solution, it appears the Department of Health and Human Services (HHS) is making some traction in assisting its own agencies and private stakeholders in confronting cyber threats. We must make sure that HHS has the resources it needs to develop and implement a robust cybersecurity strategy—something I hope we can explore today.

Just this past week, an HHS task force released a long-awaited report that describes challenges and makes recommendations to address cyber threats facing the health care sector.

The task force determined that the health care sector must pay “immediate and aggressive attention” to cybersecurity. It also made a host of important recommendations for the health care industry and HHS to consider.

There are no easy solutions for the issues highlighted in the report. I look forward to hearing how the administration intends to address them – and, importantly, how this Committee intends to hold HHS accountable for progress, or lack of progress, on this issue.

I am also interested in learning about how HHS plans to develop its newly proposed Health Cybersecurity and Communications Integration Center, and what challenges it faces in establishing and operating it.

Finally, Mr. Chairman, I am interested in understanding whether HHS has the budgetary resources it needs to appropriately address its cybersecurity responsibilities. This includes efforts to prevent cyberattacks. It also includes the HHS’s responsibilities to hold regulated entities accountable, especially when those entities fail to protect the sensitive health care information that we trust them to safeguard.

In conclusion, Mr. Chairman, we need to up our game if we intend to defend against a growing number of cyberattacks facing the health care sector.

I am pleased to welcome our witnesses from HHS, and I look forward to hearing from them about how HHS can enhance our health cybersecurity. But that being said, I believe we still have a long way to go to improve our preparedness in this area, and I look forward to hearing how this Committee intends to hold HHS accountable moving forward.

Thank you and I yield back.

###
