MICHAEL T. McCAUL, TEXAS
CHAIRMAN

BENNIE G. THOMPSON, MISSISSIPPI
RANKING MEMBER

One Hundred Fifteenth Congress
U.S. House of Representatives
Committee on Homeland Security
Washington, DC 20515

May 16, 2017

The Honorable John Ratcliffe
Chairman, Cybersecurity & Infrastructure Protection
Committee on Homeland Security
Washington, DC 20515

The Honorable Dan Donovan
Chairman, Emergency Response, Preparedness, and Communications
Committee on Homeland Security
Washington, DC 20515

Dear Chairmen Ratcliffe and Donovan:

Since last week, the "WannaCry" ransomware attacks has been crippling hospitals, utilities, telecommunications, manufacturers, transportation systems, and other critical service providers in over 150 countries across the globe. As a result, doctors were forced to treat patients without access to medical histories, medical procedures were cancelled, and some hospitals had to turn sick people away. Over the weekend, we learned that U.S. institutions were among those affected.

In the wake of this event, we believe it is crucial that our Subcommittees hold a hearing to examine the cybersecurity posture of our healthcare sector, and the security and resilience of emergency services, emergency communications, transportation and energy systems upon which the healthcare sector relies. For these "lifeline sector" systems, a failure or disruption could mean the difference between life and death.

For years, the Department of Homeland Security (DHS) has forecast a rise in cyber attacks against law enforcement, fire departments, and other providers of emergency services.[1] We have seen 9-1-1 call centers targeted, including an incident last October when centers in a dozen states were paralyzed by botnet attacks. A few months ago, the Department of Energy (DOE) reported

[1] (U//FOUO) DHS Intelligence Assessment: *Cyber Targeting of US Emergency Services Sector Limited, But Persistent* (September 24, 2015).

that the "the U.S. grid faces imminent danger from cyber attacks."[2] This is a bold prediction that the Committee on Homeland Security cannot afford to ignore.

In its sector-specific plan developed pursuant to Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience* (PPD-21), the Healthcare and Public Health Sector recognizes that it "could not function without resources and services provided by many other sectors, in particular, the so-called 'lifeline functions' – transportation, communications, energy, and water – as well as emergency services. These sectors provide necessary goods and services that support nearly every home and business across the country, are commonplace in everyday life, and are critical to disaster response and community resilience."

As such, our Committee needs to hear from the health care community, emergency services providers, and other lifeline sector representatives to learn what obstacles they face in securing their systems and maintaining continuous operations in the event of a cyber-attack. We request that the Subcommittees hold such a hearing promptly.

Thank you for your attention to this request. If you or your staff have any questions regarding this request, please contact Alison Northrop, Chief Counsel for Oversight, at 202-226-2616.

Sincerely,

CEDRIC RICHMOND
Ranking Member
Subcommittee on Cybersecurity & Infrastructure Protection

DONALD PAYNE, JR.
Ranking Member
Subcommittee on Emergency Preparedness, Response, & Communications

cc: The Honorable Michael T. McCaul, Chairman, Committee on Homeland Security
The Honorable Bennie G. Thompson, Ranking Member, Committee on Homeland Security

[2] Department of Energy, "Quadrennial Energy Review – Transforming the Nation's Electricity System: The Second Installment of the QER" (Jan. 2017), p. 405.