Testimony of Dave Summitt
H. Lee Moffitt Cancer Center & Research Institute

Before the Subcommittee on Communications and Technology
of the Committee on Energy and Commerce

"Legislating to Stop the Onslaught of Annoying Robocalls"

April 30, 2019

Good morning Chairman Doyle and members of the committee. Thank you for your invitation and providing me with the opportunity to provide information and insight to the committee on this increasingly problematic topic. It is an honor to appear before you.

My name is Dave Summitt. I am a fellow of the Institute of Critical Infrastructure Technology and I am employed as the Chief Information Security Officer over-seeing the cyber security operations for the H. Lee Moffitt Cancer Center and Research Institute located in Tampa, Florida. Moffitt provides oncology care to more than 60,000 individual patients each year, making it the third busiest stand-alone cancer hospital in the United States. Moffitt is also one of forty-nine National Cancer Institute's Designated Comprehensive Cancer Centers. This distinction is earned by demonstrating excellence in conducting scientific research and translating it into more effective cancer treatments and prevention methods. The organization is driven by excellence and it is my privilege to be part of this outstanding institution.

I am here today not only on behalf of Moffitt but also for numerous other health-related organizations that have signed on with us to endorse your efforts in addressing the serious issue before you. My ultimate goal for today's testimony is to give a voice to the hundreds of organizations that are experiencing the impact of unsolicited, fraudulent, and malicious telephone calls. When received, these calls are disruptive and potentially dangerous. Moreover, parties initiating these calls are deceptively identifying our organizations as the source, which is damaging to our reputation and, more importantly, the welfare of our communities

Every day, we are overwhelmed with new security threats and the health care sector, a United States critical infrastructure, continues to be a prime target. The health and livelihood of millions of Americans are at stake when the security of medical and financial records is compromised and healthcare operations are interrupted or shut-down.

For this reason, we greatly appreciate the efforts driven by members of the U. S. House of Representatives to address the threats posed by the malicious use of robocalls and other telephone-calling methods to gain access to, and fraudulently use sensitive data from consumers and businesses.

In our experience, this activity constitutes a serious threat to patient care, in addition to disrupting business operations and facilitating financial fraud. In recent months, many consumers, including some patients and their families, have been targeted by robocallers who use "spoofed" numbers identical to the hospitals in an effort to gain sensitive information. Even more concerning is that this practice can jeopardize the line of communication between health providers and patients by casting doubt on the integrity of calls coming from the hospital or their care provider.

What I bring to the committee is information that elevates this issue beyond the level of just an "annoyance"; these are outright fraudulent calls with malicious intent. The core problem is that calls are permitted to originate with deceptive information making the Caller ID product ineffective. The term "robocall" is generally associated with marketing firms attempting to solicit you for their product by automatically stepping through a database of phone numbers. Robocalling is only the tip of the proverbial iceberg.

Respectfully, I am not minimizing the frustration this causes for the individual consumer. In fact, on my personal cell phone I have forty-five blocked numbers entered just in the last ninety days. However, as the Chief Information Security Officer of a large organization, it rises to a much higher level than just an annoyance. They use a common cyber-attack technique called "social engineering." This relies heavily

on human interaction to trick people into letting their guard down and breaking standard security practices. When successful, social engineering attacks enable attackers to gain legitimate, authorized access to confidential information. These SPAM calls are the equivalent to SPAM emails, where the sender hides behind a façade that seems legitimate, but in reality can be an attempt to cause harm or obtain financial gain.

I am presenting to the committee three situations that represent the greatest concern for our organization. First, we receive calls that are made to look like they are coming from within our organization. Our employees see our own number on their caller ID and give no thought to answering, only to be speaking with someone with malicious intent. Second, there are calls going out to individuals across the nation where the caller ID indicates it is coming from Moffitt Cancer Center. When the recipient answers, they are greeted with someone identified as Moffitt personnel who then proceeds to ask for insurance or other payment information. The third types of call we receive are targeting specific individuals to obtain confidential information, a form of spear phishing. These calls are identified as a reputable source, such as law enforcement or a government entity, which is what heightens the likelihood of success.

To amplify the extent of this problem, I am sharing data from our organizational phone system for the past ninety days. During this time period we received over 6,600 external calls identified as a Moffitt internal phone number consuming a total of 65 hours of response time. Also concerning is that in one recent 30 day period, over 300 calls were made to Moffitt Cancer Center coming from the Washington DC area. Over half of these calls were from numbers that represented some form of federal agency identity; some were legitimate but most were not. In one recent example, the fraudulent calls that impacted Moffitt were identified as coming from the U.S. Department of Justice using a legitimate phone number. When our employees answered the phone, they were subjected to an urgent request by

the caller who self-identified as a DOJ employee. They demanded to speak with the named physician - and only that physician - and communicated an urgent problem affecting his medical license number and his Drug Enforcement Agency number. These attempts occurred over several weeks and involved numerous care providers. These calls can be quite disturbing and disruptive, and we, along with other organizations have to manage them on a daily basis.

By enacting strong consumer protections and empowering the FCC with strong enforcement tools to rein in this damaging activity, we believe that HR946, the Stopping Bad Robocalls Act could help curb these abusive practices. We also commend HR 721, the Spam Calls Task Force Act, which would establish an interagency working group to devise ways to address this threat through enforcement and regulation. I am encouraged to know that the committee is also considering other worthwhile legislation submissions.

As this Committee considers new legislative and regulatory strategies to address these issues, I would ask that three things be considered: First, place provisions for accurate caller identification into your requirements; Second, place some of this burden and responsibility back onto the telecom carriers and third; provide requirements for telecoms to work with businesses in shutting down or investigating malicious activity, especially when it involves a critical infrastructure.

My request for strengthening accountability and cooperation by telecommunications carriers is based on recent interactions in our fight against malicious activity. During two recent incidents, we contacted our carrier for assistance and received inadequate support. During the aforementioned U.S. Dept of Justice event, the telecommunications carrier told us that we needed twenty to twenty-five calls within a 72 hour window before we could file a complaint with them. The carrier's internal investigations group had defined this threshold independently on the impact it had on our operations. During a second incident, when we were investigating numerous malicious calls identified with our own organization's

number, the carrier would not give us the source of the calls and stated a subpoena would be necessary to obtain the information. I am rather astonished that others can use our owned phone number range, fraudulently represent our organization, and we have no recourse other than court order. There should be provisions made that when a company is actively investigating a suspected fraud or information security breach, they should have cooperation from the carrier. Our health care regulations require us to protect patient privacy and safety, yet it seems bad actors are more easily protected from privacy than those already covered under regulatory requirements. We are living in a high-tech age and capabilities already exist to remedy this situation, but they are not being employed. When a person receives a call identified as the "U.S. Dept of Justice", is it unreasonable to expect that it is originating from a legitimate source and not a malicious actor falsely using this identify? Borrowing a phrase from Chairman Doyle's opening statement in last month's markup meeting of H.R. 1644, you have an opportunity to "put in place 21st Century rules for a 21st Century" technology.

Moffitt and the following organizations offer our support for your efforts to curb telecommunication malicious activity. Furthermore, we hope you will count us as a resource to assist you in protecting the critical health care infrastructure. These organizations cover nine states and the DC area:

From Ranking Member Rep. Latta's state of Ohio: Genesis Health System

From committee member Rep. Soto's state of Florida:
Tampa General Hospital, Baycare Health System, Orlando Health, Apex Digital Imaging and Security Compliance Associates

From committee member Rep. Clarke's state of New York
Wellspan Health, Memorial Sloan Kettering Cancer Center and Nicholas H. Noyes Memorial Hospital

From committee member Rep. Butterfield's state of North Carolina: New Hanover Regional Medical Center

Yale New Haven Health System – Connecticut

Premise Health – Tennessee

Faith Regional Health Services - Nebraska

College of Healthcare Information Management Executives – Michigan

Institute for Critical Infrastructure Technology – Washington DC

SAP National Security Services - Pennsylvania

Thank you for your time and attention.