Chairman Thune, Ranking Member Nelson, and distinguished Committee members,

My name is Sri Sridharan, and I am the Director of the Florida Center for Cybersecurity hosted at the University of South Florida. Thank you for inviting me to provide testimony on Cybersecurity Vulnerabilities - Lessons Learned from Spectre and Meltdown.

While the Meltdown and Spectre vulnerabilities are ostensibly the topic of today's hearing, the truth is, in the world of cybersecurity, they are old news. They have been discovered, researched, and patched. What they represent, however, is something of far greater concern: the multitude of unknown vulnerabilities that most assuredly still lurk in cyberspace, waiting to be discovered and potentially exploited by cyber thieves, especially foreign nation-states. This, of course, poses a threat to our national security.

The Meltdown and Spectre vulnerabilities existed for twenty years, built into the chip design. It took us twenty years to discover a vulnerability that affects nearly every modern operating system and the most popular computer processors, used in millions of devices. Unfortunately, we have no way of knowing if it was, in fact, the researchers who found it first. The attacks that exploit these vulnerabilities are difficult to detect. A foreign threat actor could have quietly exploited one or more of these vulnerabilities without our knowledge, and they could have been doing so for twenty years.

And, although the vulnerabilities are now known, we are still not safe because, statistically, at least 25 percent of users do not apply the patches needed to mitigate these vulnerabilities. That's what we saw with the WannaCry ransomware attack last summer. Microsoft discovered a vulnerability and issued a patch in March 2017, however not everyone updated their systems. On May 12, 2017, foreign nation-state threat actors unleashed a ransomware attack designed to exploit that vulnerability that infected 300,000 computers in 150 companies and even interrupted the operations of Britain's National Health Service. One month later, despite worldwide media attention and additional updates from Microsoft, another foreign nation-state—later identified as Russia—used the same vulnerability to attack computers in several countries including the U.S., with most infections targeted at Ukraine.

My point is that Meltdown and Spectre, WannaCry and NotPetya, are symptoms of a much larger problem: cybersecurity is a race with no finish line. The question is not 'if' vulnerabilities exist. They do. They are out there, and as fast as we discover and patch them, new ones are introduced. It is simply the nature of rapidly advancing technology. The real question is: who will find it first?

We are living in the Information Age. Our information, our currency, our medicine, our economy and our secrets are digitized, and so is our conflict. Some recent headlines:

- *Cyberscoop*, June 2017, "How China's cyber command is being built to supersede its U.S. military counterpart;"
- *The Independent*, January 2018, "Cyberwarfare with Russia 'now greater threat than terrorism,' warns British Army chief;"
- *The Hill*, June 2018, "North Korea's nuclear threat is nothing compared to its cyber warfare capabilities."

In other words, these nation-state threats have already fired the first shots of cyberwarfare with the United States. We must act now to ensure that our cybersecurity forces—military, public and private—are prepared to win these battles.

How do we do that? How can we make sure that it is our researchers who discover vulnerabilities rather than foreign threat actors? How can we ensure that the United States remains the world's leading cyber power?

The answer is people. I'm sure everyone here is aware of the well-publicized difficulties the Department of Homeland Security has been facing in hiring skilled cybersecurity workers.

- *Federal News Radio*, May 2016, "DHS sweetens cyber workforce recruiting with new bonuses;"
- *Fed Manager*, October 2017, "DHS Staffing Woes, Cybersecurity Preparedness Highlighted In Hearing;" and more recently, in April 2018,
- *The Hill* reported, "DHS chief on unfilled cybersecurity positions: We're working on it."

We need to work harder and faster. We need more programs, more camps, more competitions that educate kids and inspire them to pursue cybersecurity careers. We need to create a clear path from education to employment so that people of all skill levels can easily transition into cybersecurity careers. Indeed.com reports the current median salary for an entry-level information security analyst at $80,908. The national average entry-level salary is $45,361 (iCIMS, *The Class of 2017 Job Outlook Report*). If you build it, they will come. But people need to know these opportunities exist, which brings me to my final topic: communication.

I would like to take a moment to commend the fine work of the researchers who discovered Meltdown and Spectre and their efforts in alerting manufacturers and the public. However, I wish to caution everyone here that I believe luck played a large role in avoiding disaster. Quoting from "Meltdown," a paper written jointly by the three teams that made this discovery, "We would like to thank Anders Fogh for fruitful discussions at BlackHat USA 2016 and BlackHat Europe 2016, which ultimately led to the discovery of Meltdown" (meltdownattack.com/meltdown.pdf, p. 15). BlackHat is one of the world's largest—and most notorious—information security events in both the U.S. and Europe. It is notorious because it attracts not only distinguished academics and industry professionals, but also experts with, let's say, a flexible moral code.

It was reported that researchers first alerted Intel on the afternoon of December 3, a Sunday. I applaud their sense of urgency, but must ask, at what point was the National Security Agency or the Department of Homeland Security notified? An article written by *The Verge* chronicling the discovery and disclosure of Meltdown and Spectre reads, "Perhaps most alarming, some crucial outside response groups were left out of the loop entirely. The most authoritative alert about the flaw came from Carnegie Mellon's CERT division, which works with Homeland Security on vulnerability disclosures. But according to senior vulnerability analyst Will Dormann, CERT wasn't aware of the issue until the Meltdown and Spectre websites went live, which led to even more chaos."

These two moments reveal a critical issue: the lack of a clear, rapid report-and-respond mechanism for national cybersecurity threats. Currently, multiple agencies and organizations bear responsibility for national cybersecurity defense: DHS, NSA, the military, the FBI. To which of these organizations should the researchers have reported their discovery? Do they have duty to report? When a vulnerability is reported, what is the mechanism to alert critical areas of our government?

In the case of Spectre and Meltdow, industry responded quickly with patches and solutions, but only after they were made aware of the problem. We can get a better handle on cyber hacks and breaches if we are more proactive than reactive. To this end, we need:

- A larger Cybersecurity workforce (we are dealing with a severe shortage today)
- Create awareness, provide education and training to businesses and citizens and teach them to practice good cyber hygiene
- Better coordination and dissemination of critical information (attacks, discoveries, patches et al)
- To empower and hold accountable certain government organizations that can navigate through the complex and beauracratic process
- To act with a sense of urgency
- To let the government play a major coordinating role

Chairman Thune, Ranking Member Nelson, and esteemed Committee members, I thank you for allowing me to share my thoughts, and I look forward to answering your questions.