To: Clients
From: GoldsteinCope Policy Solutions
Date: July 19, 2018
Title: Senate Committee on Commerce, Science, and Transportation hearing entitled "Complex Cybersecurity Vulnerabilities: Lessons Learned from Spectre and Meltdown"

I. Executive Summary:

On Wednesday, July 11, 2018 at 10:00am, the Senate Committee on Commerce, Science, and Transportation held a hearing to examine the discovery of and response to the Spectre and Meltdown cybersecurity vulnerabilities. During their opening statements, the witnesses outlined the process by which industry responds to the discovery of new cyber vulnerabilities and discussed their efforts to respond to the Spectre and Meltdown vulnerabilities in early 2018. During question and answer, the Senators in attendance were particularly interested in public-private partnerships to respond to cyber vulnerabilities.

II. Senators in Attendance:

Chairman John Thune (R-SD)
Senator Roger Wicker (R-MS)
Senator Cory Gardner (R-CO)

Ranking Member Bill Nelson (D-FL)
Senator Richard Blumenthal (D-CT)
Senator Ed Markey (D-MA)
Senator Tom Udall (D-NM)
Senator Maggie Hassan (D-NH)

III. Opening Statements:

A. Chairman Thune

Chairman Thune began his opening statement stating that cyber criminals in rogue states routinely attempt to infiltrate the United States' critical infrastructure and that it is the Federal government's responsibility to prevent these attacks. He stated that "white hat" security researchers recently found two particularly serious cyber vulnerabilities: the Spectre and Meltdown vulnerabilities. Chairman Thune stated that these vulnerabilities took too long to disclose to the public and raise the issue of how coordinated vulnerability disclosures may be improved in the future. He continued, stating that Huawei, a Chinese company, was informed of these vulnerabilities before the U.S. Government and before they became public. Chairman Thune expressed his belief that a better coordinated disclosure process between industry and the Federal government would have protected consumers and national security more effectively. Chairman Thune concluded his opening statement by expressing his belief that public-private partnerships must lead the enhancement of U.S. cybersecurity protections.

B. Ranking Member Nelson

Ranking Member Nelson began his statement saying that he has gradually realized cybersecurity vulnerabilities are some of the most serious threats to the U.S. Federal government and the security of American society at large. He expressed his belief that cybersecurity threats will intensify in the future, including attacks against U.S. elections. He continued, stating the discovery of the Spectre and Meltdown vulnerabilities should be a wakeup call to the United States and expressed his belief that the country is unprepared to deal with these near-existential threats. He stated that not only criminals but also nation states will exploit these vulnerabilities in the future. He lamented the fact that chipmakers failed to notify the U.S. government of the Spectre and Meltdown vulnerabilities in a timely fashion and called this lack of disclosure "baffling and inexcusable."

IV. Witness Statements:

A. Donna Dodson (Chief Cybersecurity Advisor and Director of the National Cybersecurity Center of Excellence, National Institute of Standards and Technology (NIST), U.S. Department of Commerce)

Ms. Dodson's testimony focused on NIST's activities to address the Spectre and Meltdown vulnerabilities. She testified that NIST works to identify, understand, and combat hardware vulnerabilities and lead industry and government responses to them. Ms. Dodson said mitigating the effects of these types of vulnerabilities requires a multipronged effort, including comprehensive public-private partnerships to respond to effectively and patch vulnerabilities. Continuing, Ms. Dodson stated NIST continues to develop industry guidelines to protect confidential information and the integrity of U.S. computer systems. She expressed her belief that NIST's guidelines have already improved the cyber resiliency of the U.S. government and domestic industry and that the Institute will continue to do so in the future.

B. Dr. José-Marie Griffiths (President, Dakota State University)

Dr. Griffiths began her testimony stating the internationalization of the processor supply chain has significantly complicated the United States' ability to respond effectively to cyber vulnerabilities. She said that the United States should develop comprehensive guidelines to manage the future discovery of cybersecurity vulnerabilities. She stated a coordinated effort across the industry, with the help of the U.S. government, would best protect U.S. consumers in the future. Next, she said that Congress must delegate response authority to a centralized actor who could manage the entire response process to the discovery of a cybersecurity vulnerability. In addition, Dr. Griffiths testified that the U.S. must improve cybersecurity education in the United States to leverage the country's significant human resources and develop a comprehensive domestic cybersecurity industry.

C. Joyce Kim (Chief Marketing Officer, ARM)

Ms. Kim's testimony focused on ARM's handling of Spectre and Meltdown. She stated that ARM designs processors and those designs are licensed to chip manufacturers. She continued, expressing her belief that Spectre and Meltdown were unprecedented challenges to the microprocessor industry. Ms. Kim continued, testifying that within ten days of notification, ARM was working with its customers to develop mitigations to the disclosed vulnerabilities. Moreover, the company published research and created a public website to increase the public's awareness of Spectre and Meltdown. She stated that the company promptly notified the U.S. government and chose to avoid public disclosure until after ARM could patch customers' vulnerabilities. She concluded her statement saying that ARM will continue to work with the U.S. national security community to better protect the United States from cyber-attacks.

D. Art Manion (Senior Vulnerability Analyst, CERT Coordination Center, Software Engineering Institute, Carnegie Mellon University)

Mr. Manion's testimony focused on responding to complex cybersecurity vulnerabilities. He testified that in 2017, over 20,000 system vulnerabilities were publicly disclosed. He described the response practices to newly discovered cyber vulnerabilities: first, someone must discover the vulnerability and report it to a vendor. Next, an analysis of the vulnerability must take place in order to determine a fix. Then, industry will attempt to patch the issue before ultimately publicly disclosing the vulnerability. Mr. Manion said the steps are kept secret to avoid bad actors exploiting the vulnerabilities, such as when the "Wannacry" virus swept across the globe. He stated that the need for secrecy increases the complexity of the process, as industry must decide whom to tell about the vulnerabilities and when. He concluded that the Spectre and Meltdown response process went relatively well but that adjustments to more quickly inform relevant stakeholders would be beneficial in the future.

E. Sri Sridharan (Managing Director, Florida Center for Cybersecurity, University of Florida)

Mr. Sridharan stated that the Spectre and Meltdown vulnerabilities existed for 20 years and that they were present in millions of computers around the world before they were discovered. He stated that foreign bad actors could have been exploiting the vulnerabilities for that entire duration. He expressed his belief that these two vulnerabilities, and their eventual discovery, were simply symptoms of a larger problem. He testified that the United States must act decisively to prepare the country for an inevitable cyberwar. To do so, he recommended the United States invest in cybersecurity education. Next, echoing Dr. Griffith's recommendation, Mr. Sridharan said that the United States needs to streamline cybersecurity vulnerability response practices so industry can have one contact in the Federal government with whom to work.

GoldsteinCope Policy Solutions

V. Question & Answer:

A. Public-Private Coordination

Chairman Thune asked how the Federal government and private industry can better coordinate their response to the discovery of cybersecurity vulnerabilities. **Mr. Manion** testified that the current coordination and response standards are generally effective but that the execution of the plans could be improved.

B. Responding to Spectre and Meltdown

Chairman Thune asked **Ms. Kim** what ARM has learned from their response to Spectre and Meltdown. She stated ARM has intensified engagement efforts with the cybersecurity research community to better understand potential cybersecurity vulnerabilities. Moreover, **Ms. Kim** stated that the company will seek to better coordinate with government stakeholders in the future.

Ranking Member Nelson stated that Intel notified Chinese companies of the Spectre and Meltdown vulnerabilities before notifying the U.S. government. **Senator Nelson** asked **Ms. Kim** how ARM handled the same situation. **Ms. Kim** stated that ARM notified Chinese companies before public disclosure. **Mr. Manion** expressed his belief that informing the U.S. government seven months after notifying customers was a mistake.

Senator Hassan asked if the Spectre and Meltdown vulnerabilities have been completely patched. **Ms. Kim** stated that, in many instances, mitigations and patches are developed to reduce vulnerabilities. She stated that the problem had not been completely patched but that it would be extremely complex to take advantage of remaining vulnerabilities. **Ms. Dodson** stated that NIST believes they will be dealing with vulnerabilities related to Meltdown and Spectre for several years.

C. Other Cybersecurity Vulnerabilities

Senator Gardner asked **Ms. Dodson** if the United States government is currently buying unsecure devices. **Ms. Dodson** stated that the government is buying unsecured devices. She continued, testifying that the U.S. government needs to improve cybersecurity practices.

Senator Markey asked if creating cybersecurity certification regimes would be beneficial to improving the cyber hygiene of Internet of Things (IoT) devices. **Mr. Manion** expressed his belief that providing more cybersecurity information to the consumer, such as a cybersecurity certification, would be beneficial to consumers' security.