Testimony of
Joyce Kim
Chief Marketing Officer, Arm
before the
United States Senate
Committee on Commerce, Science, and Transportation
Hearing on
Complex Cybersecurity Vulnerabilities: Lessons Learned from Spectre and Meltdown
July 11, 2018

Good morning. Chairman Thune, Ranking Member Nelson, and members of the Committee I would like to thank you for holding this hearing and for inviting Arm to participate. My name is Joyce Kim and I am the Chief Marketing Officer for Arm. Arm is the leading global provider of processor designs for mobile devices, the Internet of Things, and advanced computing. It is highly likely you are in possession of several Arm designed processors right now. If you have a mobile phone, smart watch, or tablet with you, you are utilizing Arm technology. As is well known, some of the products designed by Arm, were found to be subject to vulnerabilities known as Spectre and Meltdown. Other manufacturers' processors were also affected, reportedly far more substantially that Arm's. The Spectre and Meltdown vulnerabilities were made public on January 3, 2018. Given the prevalence of the affected technologies, we understand this Committee's and the government's interest in these vulnerabilities and the process followed to address them. I look forward to providing the Committee with information about Arms' response and our approach to addressing vulnerabilities in the highly interconnected global mobile supply chain.

As Arm's Chief Marketing Officer, it may not be readily apparent why I would be testifying today. I have more than 25 years in the tech sector, and I was heavily involved in Arm's response to the Spectre and Meltdown vulnerabilities on behalf of the executive team. This included interacting with Google Project Zero, after it found the vulnerabilities, coordinating with other industry companies that were addressing the vulnerabilities, as well as Arm's customers and partners to put mitigations and supporting documentations in place.

Arm treated and responded to these vulnerabilities with the utmost urgency and seriousness. We responsibly verified the issues within days of notification and successfully worked to mitigate the issues over several months. Despite these efforts, I believe many press stories on these vulnerabilities sensationalized the issue. This is not unusual when it comes to security vulnerabilities. Nonetheless, information about the Meltdown and Spectre vulnerabilities was handled with discretion and care by Arm due to the potential malicious exploitation of this vulnerability. As a general matter, Arm believes that vulnerability information is sensitive and should be treated with caution. Often, when vulnerabilities are discovered by security researchers, they will notify affected parties and provide time to develop solutions and mitigations before broader public disclosure. The length of time depends on the severity of a vulnerability, availability of a solution or mitigation, the complexity of developing such solutions, and potential impact of early disclosure. Having been involved in coordinating Arm's

response to these vulnerabilities from days after the discovery in June 2017, I can attest that addressing these vulnerabilities was a top priority for Arm's senior leadership and senior technical staff. I am pleased to be testifying today to share Arm's perspective on the efficiency and effectiveness by which we worked with our partners to respond to these vulnerabilities.

Arm's business is to design processors that are used in a variety of devices and equipment
To understand Arm's role in responding to the Spectre and Meltdown vulnerabilities, it may be helpful to start with a brief overview of Arm's business. Arm creates processor architectures that are primarily licensed to semiconductor manufacturers. Arm has two distinct types of commercial relationships with its direct customers for processor technology:

- "Implementation partners" license processors that have been fully designed, developed, and implemented by Arm itself. These partners then manufacture their own resulting chips.

- "Architecture partners" license Arm's processor architecture, but they design, develop, and implement their own processors based upon Arm's architectures. The architecture partners develop processors that, while software compatible, are proprietary in their implementation, and the specific detailed knowledge of the processors is not within Arm's knowledge or control. These partners then manufacture their own resulting chips.

Arm does not sell a physical product that is utilized by end users, nor do we have direct business relationships with end users or most of the software providers and supply chain. We license intellectual property in the form of processor designs to our customers who may or may not have a direct relationship with end users. Therefore, our response and mitigation plans to the Spectre and Meltdown vulnerabilities required a collaborative approach, including not only our architecture and implementation partners, but other software providers and industry.

Arm's exposure to the Spectre and Meltdown vulnerabilities was relatively limited
Spectre and Meltdown are vulnerabilities that take advantage of a design feature intended to improve the performance of processors. The vulnerabilities were discovered in a new area of research exploring the theoretical possibility of utilizing that performance feature, known as speculative execution, as a mechanism to extract pieces of sensitive data through a side-channel attack.

It should be noted that possible exploitations would be difficult, insofar as they appear to be dependent on malware running locally, which would have to be deployed on the target device. This means a device must already be compromised to execute this type of attack. It is therefore imperative for users to practice good security hygiene by keeping their software up-to-date and avoiding suspicious links or downloads. Arm has emphasized this in the process of developing and promoting mitigations for Meltdown and Spectre. I would also note, the vast majority of

chips based on Arm processors are not impacted by Meltdown or Spectre.[1] Nonetheless, Arm and all of our industry and business partners have taken this very seriously.

Moreover, to date, Arm has been unable to create by itself (or identify from third-parties) any proof of concept code that creates the conditions necessary to improperly extract data from a mobile system using the Spectre vulnerability on any Arm processor. Arm is not able to detect if these vulnerabilities have been exploited, but, as mentioned previously, exploitation of the vulnerability requires malicious code to be installed on the user device. Industry researchers have only seen a rise in such malicious code following the public disclosure of such vulnerabilities.[2] Because mitigations were made available by Arm prior to the public disclosure through collaboration with our customers and others in industry, Arm believes that the ability for bad actors to use such vulnerabilities will be reduced by that collaboration.

Arm responded thoroughly to the Specter and Meltdown vulnerabilities

Upon learning of the first variants of Spectre and Meltdown on June 1, 2017, Arm acted expeditiously to validate the issues and help its partners develop mitigations. That work entailed placing a priority on evaluating the vulnerability, its potential impact on processors implemented by Arm, and developing mitigations and software that its architecture and implementation partners could use and deploy to secure their devices and operating systems. In determining how to disseminate information about vulnerabilities and mitigations, Arm prioritized rapid development of technical solutions that could mitigate vulnerabilities and be used by its customers throughout the industry.

Within 10 days of learning of the potential exploits in June 2017, Arm informed architecture partners to provide them knowledge so they could evaluate the vulnerabilities with respect to their own implementations of the Arm architecture. This is due to the points mentioned above about Arm's business relationship with these customers. Arm's architecture partners create custom designs compliant with the Arm architecture licensed to them, so we are unaware how, or if, the end product these customers create may be affected by these vulnerabilities. We informed our implementation partners and provided appropriate mitigations in January 2018. Arm notified this set of partners later because the company knew that implementation partners would be affected and would not need to create their own mitigations because they receive processors designed by Arm, rather than a license to create their own.

After the public disclosure, Arm communicated recommended mitigation measures to all affected customers. Arm publicly released a detailed technical white paper that identified the issues and mitigations. Arm has updated that white paper as appropriate. The impact of this outreach and coordination was broad, covering companies, developers, and users of Arm processors across a wide variety of business sectors and industries.

---

[1] See http://www.arm.com/security-update

[2] See *Malware Exploiting Spectre, Meltdown Flaws Emerges,* https://www.securityweek.com/malware-exploiting-spectre-meltdown-flaws-emerges

Arm's response to the variants disclosed in January 2018 was praised publicly by ArsTechnica, an online publication read widely by technologists and IT professionals. In particular, the publication stated "Arm's response was the gold standard. Lots of technical detail in a whitepaper…"[3]

Later in 2018, a fourth variant to the Specter and Meltdown vulnerabilities emerged which Arm again aggressively addressed. We again chose to notify architecture partners early in the process for the reasons discussed above. Arm was able to determine which implementation partners were affected and which were not; Arm notified affected implementation partners approximately one month before public disclosure to afford the more time to put the mitigations in place prior to public disclosure. Arm also notified the US government of Variant 4 in advance of public disclosure.

Arm has engaged the United States Government

As Arm previously stated to the Committee in our written response to Chairman Thune and Ranking Member Nelson on March 1, 2018, we did not communicate with the US Government prior to the initial Spectre and Meltdown variants being disclosed by Google Project Zero in January 2018. After considering emerging practices across industry, and after discussions with this Committee and your colleagues in the House of Representatives, Arm recognized and has pursued several process refinements to improve its handling of vulnerabilities. Among those, we have recognized the importance of working with government stakeholders that may be able to share information and help minimize the impact on end users. As such, Arm did notify the US government and brought our chief architect to DC from Arm's headquarters in Cambridge, United Kingdom to brief government stakeholders at the Department of Homeland Security (DHS) on Variant 4 in advance of the public disclosure of that vulnerability. We have remained in contact with DHS and plan further engagements to share information and best practices. We look forward to a productive and mutually beneficial relationship that can contribute to security in the mobile ecosystem.

Arm has refined its vulnerability handling process.

Again, I believe Arm handled the response to these vulnerabilities extremely well. However, there is always room for improvement, because cybersecurity risk management is a process that evolves over time. As a result, Arm has taken several steps to refine its approach to vulnerability identification and management. First, Arm has created a dedicated, externally facing website with details on how researches may contact us with potential product vulnerabilities.[4] Second, Arm has put in place an internal vulnerability handling and disclosure policy based on the International Organization for Standards (ISO) standard numbers 30111[5]

---

[3] See *Meltdown and Spectre: Here's want Intel, Apple, Microsoft, others are doing about it,* https://arstechnica.com/gadgets/2018/01/meltdown-and-spectre-heres-what-intel-apple-microsoft-others-are-doing-about-it/

[4] See https://www.arm.com/security

[5] See https://www.iso.org/standard/53231.html

and 29147[6], respectively. Lastly, as noted, Arm has engaged the US government to work collaboratively to minimize the impact of vulnerabilities on end users in advance of public disclosure of vulnerabilities.

Conclusion

Thank you again for the invitation to testify today. I look forward to your questions.

[6] See https://www.iso.org/standard/45170.html