AMD's Responses to Energy & Commerce Committee's January 24, 2018 Requests

Security is and always has been a fundamental focus for AMD, across all our products. We are vigilant about security in both our product design and throughout the product lifecycle. As new potential exploits are identified, like we have seen with Spectre and Meltdown, we are dedicated to responding with speed and focus to help keep the end users of our products protected.

1. Why was an information embargo related to the Meltdown and Spectre vulnerabilities imposed?
   AMD Response: In order to help protect end users from exploitation of potential vulnerabilities, industry practice has long been to limit sharing of such potential vulnerabilities from initial notification until public disclosure to allow time for assessment of susceptibility and development and deployment of mitigations. *See* ISO/IEC 29147 (attached).

   In this case, a researcher from Google Project Zero ("GPZ") informed us in June of 2017 of potential security vulnerabilities on central processing units ("CPUs") from AMD, Intel and ARM—later referred to as Spectre and Meltdown by a separate independent research team. Per standard GPZ practice, the researcher stated that the results would be publicly disclosed in 90 days, a date which was exclusively set by GPZ. GPZ subsequently notified us that it had extended the publication deadline to January 3, 2018 and then to January 9, 2018. We welcomed this extension because it afforded us more time to determine the potential susceptibility of our products to each of the three variants and, where applicable, to identify and develop mitigation techniques to help protect the end users of our products. (During this time period, we established our belief that unique architectural design differences do not render our CPUs susceptible to Variant 3/Meltdown.) We understand the public disclosure by GPZ on January 3, instead of January 9, to be in response to growing public awareness of the vulnerabilities.

2. What company or combination of companies proposed the embargo?
   AMD Response: Please see our response to Question 1.

3. When was the United States Computer Emergency Readiness Team (US-CERT) informed of the vulnerabilities?
   AMD Response: We did not inform the United States Computer Emergency Readiness Team ("US-CERT") of the GPZ research. We also did not report the GPZ research to the Computer Emergency Readiness Team Coordination Center ("CERT/CC"), which is a private, non-governmental organization at Carnegie Mellon University. Current guidance from the U.S. Department of Homeland Security ("DHS") provides for voluntary reporting of cybersecurity incidents and malicious software to US-CERT. Conversely, DHS guidance provides for voluntary reporting of vulnerabilities, such as those at issue here, to Carnegie Mellon University's CERT/CC. While federal civilian agencies are required to report cybersecurity incidents to US-CERT, there is no similar requirement for any entity, including private companies such as AMD, to report vulnerabilities to either US-CERT or CERT/CC.

4. When was the Computer Emergency Readiness Team Coordination Center (CERT/CC) informed of the vulnerabilities?

AMD Response: Please see our response to Question 3.

5. Did your company perform any analyses to determine whether the embargo could have any negative impacts on critical infrastructure sectors such as healthcare and energy that rely on affected products?
   AMD Response: As explained in response to Question 1, GPZ specified the date for public disclosure. We did not perform any such targeted analyses, but instead focused our efforts on assessing the susceptibility of our products to the vulnerabilities identified by GPZ and, where applicable, developing mitigations to help protect the end users of our products, including those in the healthcare and energy sectors.

6. Did your company perform any analyses to determine whether the embargo could have any negative impacts on other information technology companies that rely on affected products?
   AMD Response: As explained in response to Question 1, GPZ specified the publication date. As noted in response to Question 5, we did not perform any such targeted analyses, but instead focused our efforts on assessing the susceptibility of our products to the vulnerabilities identified by GPZ and, where applicable, developing mitigations to help protect the end users of our products, including those of other technology companies.

7. What resources or best practices did your company use in deciding to implement the embargo?
   AMD Response: As explained in response to Question 1, GPZ specified the publication date. We did not establish the initial 90-day publication time frame or subsequent publication deadlines of January 3, 2018 and January 9, 2018. However, we welcomed the time that GPZ provided because it permitted us to work diligently on our vulnerability assessment and development of our mitigation plan.

8. What resources or best practices did your company use in implementing the embargo itself?
   AMD Response: As explained in response to Question 1, GPZ specified the publication date. Upon receipt of the initial communication from the GPZ researcher and continuing through today, we have leveraged ISO/IEC 29147 for assessing and mitigating potential security vulnerabilities.

9. Based on your company's experience during this process, has your company established lessons learned relating to multi-party coordinated vulnerability disclosure?
   AMD Response: We are currently focused on continuing research on the potential vulnerabilities and deployment of software and microcode to mitigate risk to the end users of our products. We intend to assess AMD’s processes for evaluating and addressing potential security vulnerabilities and will continue to look for opportunities to strengthen those processes.