February 7th, 2018

The Honorable Greg Walden
United States House of Representatives
2125 Rayburn House Office Building
Washington, DC 20515-6115

Dear Chairman Walden, Chairman Blackburn, Chairman Latta, and Chairman Harper,

Thank you for your letter of January 24, 2018. We welcome the opportunity to address your questions about our approach to and practices regarding technological vulnerabilities such as the ones you mention.

Security is a top priority for Google. In 2014, Google formed a new team called Project Zero. Brought together by their expertise and a belief that the Internet should be safer for everyone to use, Project Zero's security researchers have made it their mission to use public research and vulnerability disclosure to significantly reduce the number of people harmed by targeted attacks, with a particular focus on so-called zero-day vulnerabilities.

Project Zero is committed to transparency, and every vulnerability discovered by the team is filed in a database accessible to the public. In this case, Project Zero approached the Meltdown and Spectre vulnerabilities according to Google's vulnerability disclosure policy and process. We describe this policy and process and more in our responses to your specific questions below.

1. **Why was an information embargo related to the Meltdown and Spectre vulnerabilities imposed?**

Project Zero follows Google's 90-day vulnerability disclosure policy and process, with limited exceptions. That policy is described here: https://googleprojectzero.blogspot.com/2015/02/feedback-and-data-driven-updates-to.ht

ml and is consistent with industry standard practices whereby an entity that discovers a vulnerability notifies the developer and delays its own public disclosure of that vulnerability to allow the developer time to respond effectively and avoid its exploitation. It is a practice followed by U.S. CERT, among others.

Project Zero does not bar organizations from further distributing the information it provides to developers. Consistent with the purpose of Project Zero's 90-day vulnerability disclosure period, the Project Zero team does advise that a developer should be thoughtful about further dissemination of information to prevent premature public disclosure that can result in, among other things, actors developing exploits prior to the vulnerability being fixed.

2. **What company or combination of companies proposed the embargo?**

As discussed above, Project Zero has a standard 90-day disclosure practice that it follows upon identification of a security vulnerability. Consistent with that practice, Project Zero made disclosures of the Spectre and Meltdown security vulnerabilities to Intel, AMD and ARM. The notification stated that Project Zero would not disclose the identified vulnerabilities for 90 days, allowing the developers to fix the vulnerability before public disclosure and potential exploitation by bad actors. That disclosure date was extended over time, in consultation with the affected developers and given the complex nature of the vulnerability and the mitigations.

3. **When was the United States Computer Emergency Readiness Team (US-CERT) informed of the vulnerabilities?**

As described above, Project Zero's standard practice is to inform the developer who can fix a vulnerability discovered by Project Zero. Project Zero then defers to the developer to decide when and whether they inform others, including US-CERT.

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

As described above, Project Zero's standard practice is to inform the developer who can fix a vulnerability discovered by Project Zero. Project Zero then defers to the developer to decide when and whether they inform others, including CERT/CC.

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?**
    a. **If so, what were the results?**
    b. **If no, why not?**

Consistent with industry practice, Project Zero does not typically engage in analyses of the impact of vulnerabilities on other companies or industry sectors, and instead generally defers to those to whom we've reported to assess the impacts of, and how best to address, the vulnerabilities. While there was a general awareness that, due the nature of these vulnerabilities, there was a potential for broad impact on many industries, no formal industry analysis was conducted.

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?**
    a. **If so, what were the results?**
    b. **If no, why not?**

As described above, Project Zero does not typically engage in analyses of the impact of vulnerabilities on other companies or industry sectors, and instead generally defers to those to whom we've reported to assess the impacts of, and how best to address, the vulnerabilities. While there was a general awareness that, due the nature of these vulnerabilities, there was a potential for broad impact on many industries, no formal industry analysis was conducted.

7. **What resources or best practices did your company use in deciding to implement the embargo?**

As a leading zero-day vulnerability research organization, Project Zero routinely reviews best practices and industry standards regarding vulnerability disclosures. Some of those practices are discussed in Project Zero's blog regarding its own policies (https://googleprojectzero.blogspot.com/2015/02/feedback-and-data-driven-updates-to.html). Google's default 90-day delay is based in part on findings in Project Zero's research that considers the needs of developers to have enough time to create effective fixes for

security vulnerabilities before those vulnerabilities become public and and subject to exploitation.

Google approached the Meltdown and Spectre vulnerabilities in a manner consistent with its standard vulnerability reporting process. Ultimately, because of the complex nature of the vulnerability, as noted in your letter, the public disclosure deadlines were extended.

8. **What resources or best practices did your company use in implementing the embargo itself?**

Please see our answer to question 7 above.

9. **Based on your company's experience during this process, has your company established lessons learned relating to multi-party coordinated vulnerability disclosure?**

    a. **What are they?**

Our longstanding vulnerability reporting program is based on technical security expertise and experience in addition to Project Zero's research into best practices and standards around vulnerability disclosures. With that said, we continually improve both our vulnerability disclosure process and how we address security vulnerabilities based on what we learn from particular security incidents. We anticipate we will do so here. Our work has not ended and we continue to work on mitigation and further research in this area, in cooperation with others in industry and academia.

We appreciate the opportunity to describe in more detail how Google approaches vulnerability disclosures generally as well as in the specific cases of Meltdown and Spectre. Helping to improve the safety for all users of the Internet is deeply important to Google, and we thank you for the chance to underscore our commitment to improving security for our products and beyond.

Sincerely,

Susan Molinari
Vice President, Public Policy and Government Relations, Americas
Google

cc: Chairman Marsha Blackburn, Chairman Bob Latta, Chairman Gregg Harper