January 31, 2018

The Honorable Greg Walden
Chairman
United States House of Representatives
Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, DC 20515-6115

The Honorable Marsha Blackburn
Chairman
United States House of Representatives
Committee on Energy and Commerce
Subcommittee on Communications and
Technology
2125 Rayburn House Office Building
Washington, DC 20515-6115

The Honorable Robert E. Latta
Chairman
United States House of Representatives
Committee on Energy and Commerce
Subcommittee on Digital Commerce and
Consumer Protection
2125 Rayburn House Office Building
Washington, DC 20515-6115

The Honorable Gregg Harper
Chairman
United States House of Representatives
Committee on Energy and Commerce
Subcommittee on Oversight and
Investigations
2125 Rayburn House Office Building
Washington, DC 20515-6115

RE: Intel Corporation

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

Thank you for your letter regarding the recently disclosed security vulnerabilities dubbed "Spectre" and "Meltdown." Intel appreciates your desire to understand the facts about these recent disclosures and looks forward to continued dialogue with the Congress on the best policies for our industry going forward.

The collaboration between Intel and others in the technology industry regarding the disclosure and mitigation of these vulnerabilities was done in accordance with widely accepted principles commonly referred to as “responsible disclosure.” Responsible disclosure is based on two foundational concepts: First, when companies become aware of security vulnerabilities, they work as quickly, collaboratively, and effectively as possible to mitigate those vulnerabilities. Second, they simultaneously take steps to minimize the risk that exploitable information becomes available before mitigations are available – through leaks or otherwise – to those who would use it for malicious purposes. While one can debate the details of how best to execute responsible disclosure in specific incidents, Intel agrees with the prevailing industry view that in general responsible disclosure is the best practice because it maximizes information security while minimizing risk to end-users. Security vulnerabilities vary in their complexity and seriousness, and under responsible disclosure, Intel and other technology companies have identified and fixed many security vulnerabilities over the years. Security improvements in the form of updates and patches are a necessary and ubiquitous part of modern technology (e.g., updates to smartphones and computers are familiar to most users). The best security practice for every technology user remains to install updates as soon as they become available.

Intel strongly supports these principles of responsible disclosure, and believes the collaborative actions it and others in the industry took in the months prior to the public disclosure of these vulnerabilities enhanced the security of technology users around the world. This limited group of collaborators worked together for months to develop appropriate mitigations for these vulnerabilities, and then Intel worked with a more expanded group of customers to test and implement certain mitigations in preparation for their release to consumers. This was necessary because Intel sells primarily components, not finished computer systems, and it requires the assistance of its customers to deploy security updates to end users. As a result, by the time detailed information about these vulnerabilities was leaked to the public, before the scheduled date for public disclosure, significant mitigations were already available and in place. Before the leak, Intel disclosed information about Spectre and Meltdown only to companies who could assist Intel in enhancing the security of technology users. Intel also planned to brief governments in advance of the scheduled date for public disclosure on January 9, 2018. After the leak, Intel expedited its plans to deploy the mitigations and promptly briefed governments and others about the issues.

That is not to say our work is done. Protecting the security of our customers and end-users is an ongoing task, and even now Intel has engineers working around the clock to improve mitigations and enhance the security of our products. Intel has adopted a public pledge called the Security First Pledge, under which Intel hopes to lead the industry in transparency around these issues. Intel embraces this public role and remains committed to working non-stop to enhance technology security worldwide. Later this year, Intel will introduce new hardware design changes in our products to address vulnerabilities such as Spectre and Meltdown. Intel will continue to perform this work under the principles of responsible disclosure and Intel’s Security First Pledge, and with the overriding goal of doing everything in its power to protect technology users from cybercriminals.

Intel's answers to the Committee's specific questions are set forth below:

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

Intel was informed of these vulnerabilities in June 2017 by Google Project Zero ("Google PZ"), a team employed by Google to find security vulnerabilities. After Google PZ informed Intel and others of these vulnerabilities and prior to Google PZ's January 3, 2018 public release, a core group of industry participants began working on developing mitigations. Once those mitigations were sufficiently developed, Intel provided information about the mitigations to certain customers, including manufacturers of computers and providers of cloud services. These notifications were carefully limited to the information necessary for the customers to implement mitigations to the vulnerabilities.

The disclosure of information in this limited way was consistent with accepted principles of responsible disclosure. An initial disclosure to a limited audience allowed mitigations to be developed, and subsequent disclosure allowed those mitigations to be tested and deployed. At the same time, the restrictive nature of these disclosures helped prevent the exploitation of these vulnerabilities by malicious actors. As a result of this coordinated release of information, by early January 2018, the industry had developed and was ready to release effective mitigations. Had this type of coordinated disclosure process not been followed, there would have been a greater risk of exploitations being developed and used prior to mitigations being made available.

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

Intel was first informed of the vulnerabilities by Google PZ in June of 2017. Google PZ's standard practice is to allow vendors 90 days to develop appropriate mitigations before it releases vulnerability information publicly. In view of the time needed to coordinate the development of mitigations, Google PZ ultimately extended the disclosure timeframe for these vulnerabilities to January 9, 2018, after consultation with the companies developing the mitigations. Given that timeframe, Intel's subsequent disclosures of mitigation information to its customers were made subject to an agreement to maintain the disclosed information as confidential until January 9, 2018.

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

As explained earlier, information about the vulnerabilities was leaked in advance of the scheduled January 9, 2018 date for public disclosure. The United States Computer Emergency Readiness Team was first informed of the exploits through public disclosure on January 3, 2018. Intel promptly discussed this disclosure with US-CERT on that day and again two days later, on January 5, 2018.

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

The United States Computer Emergency Readiness Team Coordination Center was first informed of the exploits through public disclosure on January 3, 2018.

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?

Intel conducted a detailed analysis of the vulnerabilities disclosed by Google PZ in June and July 2017, and it confirmed the existence of these vulnerabilities. There was, however, no indication that any of these vulnerabilities had been exploited by malicious actors. Moreover, Intel also understood that these vulnerabilities require the execution of untrusted code in local memory and so cannot be exploited remotely or on machines that do not run untrusted code. Much of the critical infrastructure is operated by Industrial Control Systems (ICS). The generally understood characteristics of most ICS suggest that risk to these systems is likely low. Those characteristics include any of the following: (1) inability to transfer malicious code to local memory and then execute it; (2) no network connection; (3) inability to execute downloaded software or to run any software other than the built-in control program; (4) inability for multiple programs to run at once. Although ICS computers are beginning to use network connections that allow bidirectional transfer of data to facilitate remote configuration, diagnostics, and maintenance, or to interface to other parts of an enterprise, these types of connections do not generally allow for the installation of new or untrusted software and hence are also at low risk from the potential exploits. Moreover, even were any infrastructure equipment at risk, early disclosure of these vulnerabilities to maintainers of such equipment would not have enabled the more rapid development of mitigations, although it would have increased the risk of premature disclosure of these vulnerabilities.

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 discussed above, when these vulnerabilities were disclosed there was no indication of any exploitation by malicious actors. It was, therefore, consistent with widely accepted principles of responsible disclosure to engage in limited disclosure of detailed information about these vulnerabilities to certain information technology companies to enable them to help develop and implement mitigations. There was also a subsequent disclosure of information to others in the information technology industry to allow them to test deployment of those mitigations. The purpose of these limited disclosures was to allow the industry to develop and test mitigations before public release of potentially exploitable information about these vulnerabilities. Further or broader dissemination of this information to others in the information technology sector was not likely to increase the speed with which mitigations were developed and deployed, but it would have increased the risk of premature disclosure of these vulnerabilities and the development of exploitations that could have harmed information technology companies.

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

The limitations on the distribution of information used here by Intel and others in the industry are standard practice in vulnerability disclosure and incident response. Industry standards that address coordinated disclosure include ISO 29147 Information technology - Security techniques - Vulnerability disclosure,[1] the CERT® Guide to Coordinated Vulnerability Disclosure (CVD),[2] the Common Vulnerabilities and Exposures (CVE) Numbering Authority (CNA) Rules,[3] and the Forum of Incident Response Security Teams Common Vulnerability Scoring System (FIRST).[4] In addition to the standards we follow, Intel participates in numerous industry groups focused on product assurance and vulnerability handling including the Industry Consortium for the Advancement of Security on the Internet (ICASI)[5] and SAFECode.

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

The implementation of the limitation on distribution of information used in this situation was consistent with standard practice in vulnerability disclosure and incident response. Industry standards and groups that cover these practices are set forth in the prior answer.

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?

Intel continues to believe that the principles of responsible disclosure, which the industry followed in dealing with the disclosure of these vulnerabilities, provide the proper foundation for responsible handling of industry wide vulnerabilities. Disclosure of vulnerabilities should be handled in a way that maximizes the ability to develop and test mitigations before the vulnerabilities are widely available for public exploitation. That said, the response to these particular vulnerabilities has required wide-ranging cooperation and thousands of person hours across multiple companies, with more work yet to be done. Intel is in the process of distilling and analyzing the information it has obtained through this endeavor, and it expects to formulate lessons learned through that process.

* * * *

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

[2] https://resources.sei.cmu.edu/asset_files/SpecialReport/2017_003_001_503340.pdf

[3] https://cve.mitre.org/cve/cna/CNA_Rules_v2.0.pdf

[4] www.first.org

[5] www.icasi.org

Thank you again for the opportunity to respond to your questions. We look forward to discussing these issues further in our upcoming briefing.

Sincerely yours,

Greg Pearson

Global Policy Officer

GM Corporate Government Affairs

Senior Vice President