I. **US House of Representatives Committee on Energy & Commerce Inquiry**

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

    a. Intel required all information it provided related to the vulnerabilities to be subject to a Non-Disclosure Agreement that strictly controlled Amazon's use of the information. It is industry best practice to impose a confidentiality period regarding emerging security vulnerabilities to permit creation and testing of a fix, prior to public disclosure, in order to minimize risk that hackers will exploit the vulnerability.

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

    a. We understand that Google's Project Zero team disclosed the information to a limited number of hardware manufacturers, including Intel. Amazon was informed about this issue by Intel, and all information Intel provided Amazon was subject to a Non-Disclosure Agreement. The companies that discovered and initially disclosed the vulnerabilities determined the application of the Non-Disclosure Agreement. We understand that the vulnerabilities were disclosed to a limited number of companies best-positioned to develop broad, industry-wide remediation while maintaining confidentiality during the extended period required to develop countermeasures.

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

    a. We are not aware when US-CERT was informed of the vulnerabilities.

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

    a. We are not aware when CERT/CC was informed of the vulnerabilities.

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 are the results?

        i. Impositions of a confidentiality period are a common industry practice when security issues are identified, because they provide manufacturers, operating systems providers, and application developers an opportunity to develop countermeasures in advance of widespread disclosure of the issue. A limited confidentiality period was imposed to benefit many sectors, including critical infrastructure, providing manufacturers, operating system providers, and application developers an opportunity to implement countermeasures in advance of widespread disclosure of the issue.

b. If not, why not?

i. Not applicable

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 are the results?

i. We determined that a limited confidentiality period would benefit all information technology companies because it provided manufacturers, operating system providers, and application developers an opportunity to develop broadly applicable countermeasures in advance of widespread disclosure of the issue.

b. If not, why not?

i. Not applicable

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

a. Amazon complied with the Non-Disclosure Agreement that controlled the confidential information provided by Intel using Amazon's normal practices for handling confidential information.

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

a. We used our normal practices for compliance with non-disclosure agreements to prevent the unauthorized use of the confidential information. We focused our efforts on developing countermeasures for the Linux operating system and the Xen hypervisor. Countermeasures developed by AWS had broad industry application and we made them freely available to the open source Linux and Xen communities.

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?

i. We know that confidentiality periods are critical to protecting the public against new vulnerabilities. We have learned that restricting access to information under a confidentiality period is critical to successfully maintaining confidentiality while countermeasures can be implemented before the vulnerability is disclosed. This event reinforced the necessity of strict information protection, as the confidentiality period was critical to allow Intel and the Linux community the extended time required to produce countermeasures, so that when the issue was public, individuals and organizations could take the necessary steps to protect themselves.