Mr. Tim Cook  
Chief Executive Officer  
Apple, Inc.  
1 Infinite Loop  
Cupertino, CA 95014

Dear Mr. Cook:

On January 4, 2018, several companies across the information technology sector released statements addressing researchers’ discovery of two serious cybersecurity vulnerabilities affecting the companies’ products.¹ These vulnerabilities – dubbed “Meltdown” and “Spectre” – enable unauthorized access to information on systems using the affected processors, potentially facilitating the theft of sensitive data.² Considering that nearly all modern computing systems – including phones, laptops, and cloud services – rely on vulnerable chips, Meltdown and Spectre are serious vulnerabilities requiring a coordinated response.

Commendably, that coordinated response has already occurred. Affected companies began collaborating in June 2017, when researchers from Google’s Project Zero – a team dedicated to finding critical vulnerabilities such as these – informed the most heavily-impacted

companies about the vulnerabilities. Since that time, these companies have released staggered updates to their various products to mitigate the effects. More work remains to be done, however, because the vulnerabilities stem from a common and previously accepted computer engineering method. As such, full mitigation will require the rearchitecting of many chipsets. This is not a trivial problem, and will take some time to address.

We applaud the industry response and appreciate the efforts of affected companies to protect their products and users. The general consensus seems to agree that these initial efforts have mitigated the worst of the danger. Some members of the industry, however, have raised concerns about one major aspect of the response, namely the information embargo instituted by the limited number of companies originally informed about the vulnerabilities in June 2017. This embargo restricted the dissemination of information related to the vulnerabilities outside of these companies, and was meant to last from June 2017 to January 9, 2018, when most of the mitigations would be distributed, and a public announcement was planned.

However, for various reasons, information regarding both Meltdown and Spectre vulnerabilities began to leak into the public sphere prior to this planned announcement. This information – including proof-of-concept exploit code – was sufficient enough to force the companies to accelerate the termination of the embargo and move up their announcement by a week. Though this schedule adjustment has not seemed to overly impact the effectiveness of the response, it does raise questions related to the effects and appropriateness of the embargo on companies not originally included in the June 2017 disclosure, and who were caught off-guard by the January 4 announcement.

For example, some observers have raised questions about the effect of the embargo on the ability of companies not included in the original June 2017 disclosure to protect their own products and users, compared to those companies that were included. One such company, for example, stated the following, "Unfortunately, the strict embargo placed by Intel has significantly limited our ability to establish a comprehensive understanding of the potential impact." In addition, some users and companies are now reporting that some of the patches offered to address the vulnerabilities are themselves creating new problems, such as freezing patched computers or interfering with anti-virus products. As nearly all modern technology companies are impacted by these vulnerabilities, and less than ten companies were included in the original June 2017 disclosure, it is reasonable to assume that additional companies have been negatively impacted by the embargo.

While we acknowledge that critical vulnerabilities such as these create challenging trade-offs between disclosure and secrecy, as premature disclosure may give malicious actors time to

---

3 Id.
4 See supra note 1.
5 See supra note 2.
Letter to Mr. Cook
Page 3

exploit the vulnerabilities before mitigations are developed and deployed, we believe that this situation has shown the need for additional scrutiny regarding multi-party coordinated vulnerability disclosures. As demonstrated by numerous incidents over the past several years, cybersecurity is a collective responsibility. Further, it is a responsibility that is no longer limited solely to the information technology sector; connected products exist in electric grids, hospitals, manufacturing equipment, and in innumerable other sectors.

As more products and services become connected, no one company, or even one sector, working in isolation can provide sufficient protection for their products and users. Today, effective responses require extensive collaboration not only between individual companies, but also across sectors traditionally siloed from one another. This reality raises serious questions about not just the embargo imposed on information regarding the Meltdown and Spectre vulnerabilities, but on embargos regarding cybersecurity vulnerabilities in general.

Therefore, and pursuant to Rules X and XI of the United States House of Representatives, we ask that you respond to the following questions as soon as possible, but by no later than February 7, 2018:

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

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

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

4. When was the Computer Emergency Readiness Team Coordination Center (CERT/CC) 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 were the results?
   b. If no, why not?

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

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

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?

Please also arrange to provide a briefing on these issues to Committee staff by February 7, 2018. We appreciate your assistance with this request. If you should have any questions, please contact Jessica Wilkerson or John Ohly of the Majority Committee staff at (202) 225-2927.

Sincerely,

Greg Walden  
Chairman

Marsha Blackburn  
Chairman  
Subcommittee on Communications  
and Technology

Robert E. Latta  
Chairman  
Subcommittee on Digital Commerce  
and Consumer Protection

Gregg Harper  
Chairman  
Subcommittee on Oversight  
and Investigations
Mr. Jeff Bezos  
Chairman, President, and Chief Executive Officer  
Amazon  
410 Terry Ave. North  
Seattle, WA 98109

Dear Mr. Bezos:

On January 4, 2018, several companies across the information technology sector released statements addressing researchers’ discovery of two serious cybersecurity vulnerabilities affecting the companies’ products.¹ These vulnerabilities – dubbed “Meltdown” and “Spectre” – enable unauthorized access to information on systems using the affected processors, potentially facilitating the theft of sensitive data.² Considering that nearly all modern computing systems – including phones, laptops, and cloud services – rely on vulnerable chipsets, Meltdown and Spectre are serious vulnerabilities requiring a coordinated response.

Commendably, that coordinated response has already occurred. Affected companies began collaborating in June 2017, when researchers from Google’s Project Zero – a team dedicated to finding critical vulnerabilities such as these – informed the most heavily-impacted

companies about the vulnerabilities. Since that time, these companies have released staggered updates to their various products to mitigate the effects. More work remains to be done, however, because the vulnerabilities stem from a common and previously accepted computer engineering method. As such, full mitigation will require the rearchitecting of many chipsets. This is not a trivial problem, and will take some time to address.

We applaud the industry response and appreciate the efforts of affected companies to protect their products and users. The general consensus seems to agree that these initial efforts have mitigated the worst of the danger. Some members of the industry, however, have raised concerns about one major aspect of the response, namely the information embargo instituted by the limited number of companies originally informed about the vulnerabilities in June 2017. This embargo restricted the dissemination of information related to the vulnerabilities outside of these companies, and was meant to last from June 2017 to January 9, 2018, when most of the mitigations would be distributed, and a public announcement was planned.

However, for various reasons, information regarding both Meltdown and Spectre vulnerabilities began to leak into the public sphere prior to this planned announcement. This information – including proof-of-concept exploit code – was sufficient enough to force the companies to accelerate the termination of the embargo and move up their announcement by a week. Though this schedule adjustment has not seemed to overly impact the effectiveness of the response, it does raise questions related to the effects and appropriateness of the embargo on companies not originally included in the June 2017 disclosure, and who were caught off-guard by the January 4 announcement.

For example, some observers have raised questions about the effect of the embargo on the ability of companies not included in the original June 2017 disclosure to protect their own products and users, compared to those companies that were included. One such company, for example, stated the following, "Unfortunately, the strict embargo placed by Intel has significantly limited our ability to establish a comprehensive understanding of the potential impact." In addition, some users and companies are now reporting that some of the patches offered to address the vulnerabilities are themselves creating new problems, such as freezing patched computers or interfering with anti-virus products. As nearly all modern technology companies are impacted by these vulnerabilities, and less than ten companies were included in the original June 2017 disclosure, it is reasonable to assume that additional companies have been negatively impacted by the embargo.

While we acknowledge that critical vulnerabilities such as these create challenging trade-offs between disclosure and secrecy, as premature disclosure may give malicious actors time to

---

3 Id.
4 See supra note 1.
5 See supra note 2.
exploit the vulnerabilities before mitigations are developed and deployed, we believe that this situation has shown the need for additional scrutiny regarding multi-party coordinated vulnerability disclosures. As demonstrated by numerous incidents over the past several years, cybersecurity is a collective responsibility. Further, it is a responsibility that is no longer limited solely to the information technology sector; connected products exist in electric grids, hospitals, manufacturing equipment, and in innumerable other sectors.

As more products and services become connected, no one company, or even one sector, working in isolation can provide sufficient protection for their products and users. Today, effective responses require extensive collaboration not only between individual companies, but also across sectors traditionally siloed from one another. This reality raises serious questions about not just the embargo imposed on information regarding the Meltdown and Spectre vulnerabilities, but on embargos regarding cybersecurity vulnerabilities in general.

Therefore, and pursuant to Rules X and XI of the United States House of Representatives, we ask that you respond to the following questions as soon as possible, but by no later than February 7, 2018:

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

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

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

4. When was the Computer Emergency Readiness Team Coordination Center (CERT/CC) 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 were the results?
   b. If no, why not?

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

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

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?

Please also arrange to provide a briefing on these issues to Committee staff by February 7, 2018. We appreciate your assistance with this request. If you should have any questions, please contact Jessica Wilkerson or John Ohly of the Majority Committee staff at (202) 225-2927.

Sincerely,

Greg Weldon
Chairman

Robert E. Latta
Chairman
Subcommittee on Digital Commerce and Consumer Protection

Marsha Blackburn
Chairman
Subcommittee on Communications and Technology

Gregg Harper
Chairman
Subcommittee on Oversight and Investigations
Ms. Lisa T. Su
Chief Executive Officer and President
Advanced Micro Devices, Inc.
2485 Augustine Drive
Santa Clara, CA 95054

Dear Ms. Su:

On January 4, 2018, several companies across the information technology sector released statements addressing researchers’ discovery of two serious cybersecurity vulnerabilities affecting the companies’ products.¹ These vulnerabilities – dubbed “Meltdown” and “Spectre” – enable unauthorized access to information on systems using the affected processors, potentially facilitating the theft of sensitive data.² Considering that nearly all modern computing systems – including phones, laptops, and cloud services – rely on vulnerable chipsets, Meltdown and Spectre are serious vulnerabilities requiring a coordinated response.

Commendably, that coordinated response has already occurred. Affected companies began collaborating in June 2017, when researchers from Google’s Project Zero – a team dedicated to finding critical vulnerabilities such as these – informed the most heavily-impacted

companies about the vulnerabilities. Since that time, these companies have released staggered updates to their various products to mitigate the effects. More work remains to be done, however, because the vulnerabilities stem from a common and previously accepted computer engineering method. As such, full mitigation will require the rearchitecting of many chipsets. This is not a trivial problem, and will take some time to address.

We applaud the industry response and appreciate the efforts of affected companies to protect their products and users. The general consensus seems to agree that these initial efforts have mitigated the worst of the danger. Some members of the industry, however, have raised concerns about one major aspect of the response, namely the information embargo instituted by the limited number of companies originally informed about the vulnerabilities in June 2017. This embargo restricted the dissemination of information related to the vulnerabilities outside of these companies, and was meant to last from June 2017 to January 9, 2018, when most of the mitigations would be distributed, and a public announcement was planned.

However, for various reasons, information regarding both Meltdown and Spectre vulnerabilities began to leak into the public sphere prior to this planned announcement. This information— including proof-of-concept exploit code— was sufficient enough to force the companies to accelerate the termination of the embargo and move up their announcement by a week. Though this schedule adjustment has not seemed to overly impact the effectiveness of the response, it does raise questions related to the effects and appropriateness of the embargo on companies not originally included in the June 2017 disclosure, and who were caught off-guard by the January 4 announcement.

For example, some observers have raised questions about the effect of the embargo on the ability of companies not included in the original June 2017 disclosure to protect their own products and users, compared to those companies that were included. One such company, for example, stated the following, "[u]nfortunately, the strict embargo placed by Intel has significantly limited our ability to establish a comprehensive understanding of the potential impact." In addition, some users and companies are now reporting that some of the patches offered to address the vulnerabilities are themselves creating new problems, such as freezing patched computers or interfering with anti-virus products. As nearly all modern technology companies are impacted by these vulnerabilities, and less than ten companies were included in the original June 2017 disclosure, it is reasonable to assume that additional companies have been negatively impacted by the embargo.

While we acknowledge that critical vulnerabilities such as these create challenging tradeoffs between disclosure and secrecy, as premature disclosure may give malicious actors time to

---

3 Id.
4 See supra note 1.
5 See supra note 2.
exploit the vulnerabilities before mitigations are developed and deployed, we believe that this situation has shown the need for additional scrutiny regarding multi-party coordinated vulnerability disclosures. As demonstrated by numerous incidents over the past several years, cybersecurity is a collective responsibility. Further, it is a responsibility that is no longer limited solely to the information technology sector; connected products exist in electric grids, hospitals, manufacturing equipment, and in innumerable other sectors.

As more products and services become connected, no one company, or even one sector, working in isolation can provide sufficient protection for their products and users. Today, effective responses require extensive collaboration not only between individual companies, but also across sectors traditionally siloed from one another. This reality raises serious questions about not just the embargo imposed on information regarding the Meltdown and Spectre vulnerabilities, but on embargos regarding cybersecurity vulnerabilities in general.

Therefore, and pursuant to Rules X and XI of the United States House of Representatives, we ask that you respond to the following questions as soon as possible, but by no later than February 7, 2018:

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

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

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

4. When was the Computer Emergency Readiness Team Coordination Center (CERT/CC) 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 were the results?
   b. If no, why not?

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

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

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?

   Please also arrange to provide a briefing on these issues to Committee staff by February 7, 2018. We appreciate your assistance with this request. If you should have any questions, please contact Jessica Wilkerson or John Ohly of the Majority Committee staff at (202) 225-2927.

Sincerely,

Greg Walden
Chairman

Marsha Blackburn
Chairman
Subcommittee on Communications and Technology

Robert E. Latta
Chairman
Subcommittee on Digital Commerce and Consumer Protection

Gregg Harper
Chairman
Subcommittee on Oversight and Investigations
Mr. Simon Segars
Chief Executive Officer
ARM Holdings, PLC
150 Rose Orchard Way
San Jose, CA 95134

Dear Mr. Segars:

On January 4, 2018, several companies across the information technology sector released statements addressing researchers’ discovery of two serious cybersecurity vulnerabilities affecting the companies’ products.1 These vulnerabilities – dubbed “Meltdown” and “Spectre” – enable unauthorized access to information on systems using the affected processors, potentially facilitating the theft of sensitive data.2 Considering that nearly all modern computing systems – including phones, laptops, and cloud services – rely on vulnerable chipsets, Meltdown and Spectre are serious vulnerabilities requiring a coordinated response.

Commendably, that coordinated response has already occurred. Affected companies began collaborating in June 2017, when researchers from Google’s Project Zero – a team dedicated to finding critical vulnerabilities such as these – informed the most heavily-impacted

---


companies about the vulnerabilities. Since that time, these companies have released staggered updates to their various products to mitigate the effects. More work remains to be done, however, because the vulnerabilities stem from a common and previously accepted computer engineering method. As such, full mitigation will require the rearchitecting of many chipsets. This is not a trivial problem, and will take some time to address.

We applaud the industry response and appreciate the efforts of affected companies to protect their products and users. The general consensus seems to agree that these initial efforts have mitigated the worst of the danger. Some members of the industry, however, have raised concerns about one major aspect of the response, namely the information embargo instituted by the limited number of companies originally informed about the vulnerabilities in June 2017. This embargo restricted the dissemination of information related to the vulnerabilities outside of these companies, and was meant to last from June 2017 to January 9, 2018, when most of the mitigations would be distributed, and a public announcement was planned.

However, for various reasons, information regarding both Meltdown and Spectre vulnerabilities began to leak into the public sphere prior to this planned announcement. This information – including proof-of-concept exploit code – was sufficient enough to force the companies to accelerate the termination of the embargo and move up their announcement by a week. Though this schedule adjustment has not seemed to overly impact the effectiveness of the response, it does raise questions related to the effects and appropriateness of the embargo on companies not originally included in the June 2017 disclosure, and who were caught off-guard by the January 4 announcement.

For example, some observers have raised questions about the effect of the embargo on the ability of companies not included in the original June 2017 disclosure to protect their own products and users, compared to those companies that were included. One such company, for example, stated the following, "[u]nfortunately, the strict embargo placed by Intel has significantly limited our ability to establish a comprehensive understanding of the potential impact." In addition, some users and companies are now reporting that some of the patches offered to address the vulnerabilities are themselves creating new problems, such as freezing patched computers or interfering with anti-virus products. As nearly all modern technology companies are impacted by these vulnerabilities, and less than ten companies were included in the original June 2017 disclosure, it is reasonable to assume that additional companies have been negatively impacted by the embargo.

While we acknowledge that critical vulnerabilities such as these create challenging trade-offs between disclosure and secrecy, as premature disclosure may give malicious actors time to

---

3 Id.
4 See supra note 1.
5 See supra note 2.
Letter to Mr. Segars
Page 3

exploit the vulnerabilities before mitigations are developed and deployed, we believe that this situation has shown the need for additional scrutiny regarding multi-party coordinated vulnerability disclosures. As demonstrated by numerous incidents over the past several years, cybersecurity is a collective responsibility. Further, it is a responsibility that is no longer limited solely to the information technology sector; connected products exist in electric grids, hospitals, manufacturing equipment, and in innumerable other sectors.

As more products and services become connected, no one company, or even one sector, working in isolation can provide sufficient protection for their products and users. Today, effective responses require extensive collaboration not only between individual companies, but also across sectors traditionally siloed from one another. This reality raises serious questions about not just the embargo imposed on information regarding the Meltdown and Spectre vulnerabilities, but on embargos regarding cybersecurity vulnerabilities in general.

Therefore, and pursuant to Rules X and XI of the United States House of Representatives, we ask that you respond to the following questions as soon as possible, but by no later than February 7, 2018:

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

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

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

4. When was the Computer Emergency Readiness Team Coordination Center (CERT/CC) 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 were the results?
   b. If no, why not?

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

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

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?

Please also arrange to provide a briefing on these issues to Committee staff by February 7, 2018. We appreciate your assistance with this request. If you should have any questions, please contact Jessica Wilkerson or John Ohly of the Majority Committee staff at (202) 225-2927.

Sincerely,

Greg Walden
Chairman

Marsha Blackburn
Chairman
Subcommittee on Communications and Technology

Robert E. Latta
Chairman
Subcommittee on Digital Commerce and Consumer Protection

Gregg Harper
Chairman
Subcommittee on Oversight and Investigations
Mr. Sundar Pichai  
Chief Executive Officer  
Google, Inc.  
1600 Amphitheatre Parkway  
Mountain View, CA 94043

Dear Mr. Pichai:

On January 4, 2018, several companies across the information technology sector released statements addressing researchers’ discovery of two serious cybersecurity vulnerabilities affecting the companies’ products.¹ These vulnerabilities – dubbed “Meltdown” and “Spectre” – enable unauthorized access to information on systems using the affected processors, potentially facilitating the theft of sensitive data.² Considering that nearly all modern computing systems – including phones, laptops, and cloud services – rely on vulnerable chipsets, Meltdown and Spectre are serious vulnerabilities requiring a coordinated response.

Commendably, that coordinated response has already occurred. Affected companies began collaborating in June 2017, when researchers from Google’s Project Zero – a team dedicated to finding critical vulnerabilities such as these – informed the most heavily-impacted

companies about the vulnerabilities.\textsuperscript{3} Since that time, these companies have released staggered
dates to their various products to mitigate the effects.\textsuperscript{4} More work remains to be done,
however, because the vulnerabilities stem from a common and previously accepted computer
engineering method. As such, full mitigation will require the rearchitecting of many chipsets.
This is not a trivial problem, and will take some time to address.

We applaud the industry response and appreciate the efforts of affected companies to
protect their products and users. The general consensus seems to agree that these initial efforts
have mitigated the worst of the danger.\textsuperscript{5} Some members of the industry, however, have raised
concerns about one major aspect of the response, namely the information embargo instituted by
the limited number of companies originally informed about the vulnerabilities in June 2017. This
embargo restricted the dissemination of information related to the vulnerabilities outside of these
companies, and was meant to last from June 2017 to January 9, 2018, when most of the
mitigations would be distributed, and a public announcement was planned.

However, for various reasons, information regarding both Meltdown and Spectre
vulnerabilities began to leak into the public sphere prior to this planned announcement. This
information – including proof-of-concept exploit code – was sufficient enough to force the
companies to accelerate the termination of the embargo and move up their announcement by a
week. Though this schedule adjustment has not seemed to overly impact the effectiveness of the
response, it does raise questions related to the effects and appropriateness of the embargo on
companies not originally included in the June 2017 disclosure, and who were caught off-guard
by the January 4 announcement.

For example, some observers have raised questions about the effect of the embargo on
the ability of companies not included in the original June 2017 disclosure to protect their own
products and users, compared to those companies that were included. One such company, for
everything, stated the following, "[u]nfortunately, the strict embargo placed by Intel has
significantly limited our ability to establish a comprehensive understanding of the potential
impact."\textsuperscript{6} In addition, some users and companies are now reporting that some of the patches
offered to address the vulnerabilities are themselves creating new problems, such as freezing
patched computers or interfering with anti-virus products.\textsuperscript{7} As nearly all modern technology
companies are impacted by these vulnerabilities, and less than ten companies were included in
the original June 2017 disclosure, it is reasonable to assume that additional companies have been
negatively impacted by the embargo.

While we acknowledge that critical vulnerabilities such as these create challenging trade-
offs between disclosure and secrecy, as premature disclosure may give malicious actors time to

\textsuperscript{3} Id.
\textsuperscript{4} See supra note 1.
\textsuperscript{5} See supra note 2.
\textsuperscript{6} Josh Feinblum, A Message About Intel Security Findings, DIGITALOCEAN (Jan. 5, 2018),
https://blog.digitalocean.com/a-message-about-intel-security-findings/.
\textsuperscript{7} Eric Auchard & Supantha Mukherjee, Microsoft says security patches slowing down PCs, servers, REUTERS (Jan.
pcs-servers-idUSKBN1JEY17X.
Letter to Mr. Pichai

Page 3

exploit the vulnerabilities before mitigations are developed and deployed, we believe that this situation has shown the need for additional scrutiny regarding multi-party coordinated vulnerability disclosures. As demonstrated by numerous incidents over the past several years, cybersecurity is a collective responsibility. Further, it is a responsibility that is no longer limited solely to the information technology sector; connected products exist in electric grids, hospitals, manufacturing equipment, and in innumerable other sectors.

As more products and services become connected, no one company, or even one sector, working in isolation can provide sufficient protection for their products and users. Today, effective responses require extensive collaboration not only between individual companies, but also across sectors traditionally siloed from one another. This reality raises serious questions about not just the embargo imposed on information regarding the Meltdown and Spectre vulnerabilities, but on embargos regarding cybersecurity vulnerabilities in general.

Therefore, and pursuant to Rules X and XI of the United States House of Representatives, we ask that you respond to the following questions as soon as possible, but by no later than February 7, 2018:

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

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

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

4. When was the Computer Emergency Readiness Team Coordination Center (CERT/CC) 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 were the results?
   b. If no, why not?

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

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

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?

Please also arrange to provide a briefing on these issues to Committee staff by February 7, 2018. We appreciate your assistance with this request. If you should have any questions, please contact Jessica Wilkerson or John Ohly of the Majority Committee staff at (202) 225-2927.

Sincerely,

Greg Walden
Chairman

Marsha Blackburn
Chairman
Subcommittee on Communications and Technology

Robert E. Latta
Chairman
Subcommittee on Digital Commerce and Consumer Protection

Gregg Harper
Chairman
Subcommittee on Oversight and Investigations
Mr. Brian Krzanich  
Chief Executive Officer  
Intel Corporation  
2200 Mission College Blvd  
Santa Clara, CA 95054  

Dear Mr. Krzanich:

On January 4, 2018, several companies across the information technology sector released statements addressing researchers’ discovery of two serious cybersecurity vulnerabilities affecting the companies’ products.¹ These vulnerabilities – dubbed “Meltdown” and “Spectre” – enable unauthorized access to information on systems using the affected processors, potentially facilitating the theft of sensitive data.² Considering that nearly all modern computing systems – including phones, laptops, and cloud services – rely on vulnerable chipsets, Meltdown and Spectre are serious vulnerabilities requiring a coordinated response.

Commendably, that coordinated response has already occurred. Affected companies began collaborating in June 2017, when researchers from Google's Project Zero – a team dedicated to finding critical vulnerabilities such as these – informed the most heavily-impacted

companies about the vulnerabilities. Since that time, these companies have released staggered updates to their various products to mitigate the effects. More work remains to be done, however, because the vulnerabilities stem from a common and previously accepted computer engineering method. As such, full mitigation will require the rearchitecting of many chipsets. This is not a trivial problem, and will take some time to address.

We applaud the industry response and appreciate the efforts of affected companies to protect their products and users. The general consensus seems to agree that these initial efforts have mitigated the worst of the danger. Some members of the industry, however, have raised concerns about one major aspect of the response, namely the information embargo instituted by the limited number of companies originally informed about the vulnerabilities in June 2017. This embargo restricted the dissemination of information related to the vulnerabilities outside of these companies, and was meant to last from June 2017 to January 9, 2018, when most of the mitigations would be distributed, and a public announcement was planned.

However, for various reasons, information regarding both Meltdown and Spectre vulnerabilities began to leak into the public sphere prior to this planned announcement. This information— including proof-of-concept exploit code— was sufficient enough to force the companies to accelerate the termination of the embargo and move up their announcement by a week. Though this schedule adjustment has not seemed to overly impact the effectiveness of the response, it does raise questions related to the effects and appropriateness of the embargo on companies not originally included in the June 2017 disclosure, and who were caught off-guard by the January 4 announcement.

For example, some observers have raised questions about the effect of the embargo on the ability of companies not included in the original June 2017 disclosure to protect their own products and users, compared to those companies that were included. One such company, for example, stated the following, "[u]nfortunately, the strict embargo placed by Intel has significantly limited our ability to understand the full impact of these vulnerabilities." In addition, some users and companies are now reporting that some of the patches offered to address the vulnerabilities are themselves creating new problems, such as freezing patched computers or interfering with anti-virus products. As nearly all modern technology companies are impacted by these vulnerabilities, and less than ten companies were included in the original June 2017 disclosure, it is reasonable to assume that additional companies have been negatively impacted by the embargo.

While we acknowledge that critical vulnerabilities such as these create challenging trade-offs between disclosure and secrecy, as premature disclosure may give malicious actors time to

---

3 Id.
4 See supra note 1.
5 See supra note 2.
exploit the vulnerabilities before mitigations are developed and deployed, we believe that this situation has shown the need for additional scrutiny regarding multi-party coordinated vulnerability disclosures. As demonstrated by numerous incidents over the past several years, cybersecurity is a collective responsibility. Further, it is a responsibility that is no longer limited solely to the information technology sector; connected products exist in electric grids, hospitals, manufacturing equipment, and in innumerable other sectors.

As more products and services become connected, no one company, or even one sector, working in isolation can provide sufficient protection for their products and users. Today, effective responses require extensive collaboration not only between individual companies, but also across sectors traditionally siloed from one another. This reality raises serious questions about not just the embargo imposed on information regarding the Meltdown and Spectre vulnerabilities, but on embargos regarding cybersecurity vulnerabilities in general.

Therefore, and pursuant to Rules X and XI of the United States House of Representatives, we ask that you respond to the following questions as soon as possible, but by no later than February 7, 2018:

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

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

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

4. When was the Computer Emergency Readiness Team Coordination Center (CERT/CC) 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 were the results?
   b. If no, why not?

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

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

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?

Please also arrange to provide a briefing on these issues to Committee staff by February 7, 2018. We appreciate your assistance with this request. If you should have any questions, please contact Jessica Wilkerson or John Ohly of the Majority Committee staff at (202) 225-2927.

Sincerely,

Greg Walden
Chairman

Marsha Blackburn
Chairman
Subcommittee on Communications and Technology

Robert E. Latta
Chairman
Subcommittee on Digital Commerce and Consumer Protection

Gregg Harper
Chairman
Subcommittee on Oversight and Investigations
Dear Mr. Nadella:

On January 4, 2018, several companies across the information technology sector released statements addressing researchers’ discovery of two serious cybersecurity vulnerabilities affecting the companies’ products.¹ These vulnerabilities – dubbed “Meltdown” and “Spectre” – enable unauthorized access to information on systems using the affected processors, potentially facilitating the theft of sensitive data.² Considering that nearly all modern computing systems – including phones, laptops, and cloud services – rely on vulnerable chips, Meltdown and Spectre are serious vulnerabilities requiring a coordinated response.

Commendably, that coordinated response has already occurred. Affected companies began collaborating in June 2017, when researchers from Google's Project Zero – a team dedicated to finding critical vulnerabilities such as these – informed the most heavily-impacted

---


companies about the vulnerabilities. Since that time, these companies have released staggered updates to their various products to mitigate the effects. More work remains to be done, however, because the vulnerabilities stem from a common and previously accepted computer engineering method. As such, full mitigation will require the rearchitecting of many chipsets. This is not a trivial problem, and will take some time to address.

We applaud the industry response and appreciate the efforts of affected companies to protect their products and users. The general consensus seems to agree that these initial efforts have mitigated the worst of the danger. Some members of the industry, however, have raised concerns about one major aspect of the response, namely the information embargo instituted by the limited number of companies originally informed about the vulnerabilities in June 2017. This embargo restricted the dissemination of information related to the vulnerabilities outside of these companies, and was meant to last from June 2017 to January 9, 2018, when most of the mitigations would be distributed, and a public announcement was planned.

However, for various reasons, information regarding both Meltdown and Spectre vulnerabilities began to leak into the public sphere prior to this planned announcement. This information — including proof-of-concept exploit code — was sufficient enough to force the companies to accelerate the termination of the embargo and move up their announcement by a week. Though this schedule adjustment has not seemed to overly impact the effectiveness of the response, it does raise questions related to the effects and appropriateness of the embargo on companies not originally included in the June 2017 disclosure, and who were caught off-guard by the January 4 announcement.

For example, some observers have raised questions about the effect of the embargo on the ability of companies not included in the original June 2017 disclosure to protect their own products and users, compared to those companies that were included. One such company, for example, stated the following, "Unfortunately, the strict embargo placed by Intel has significantly limited our ability to establish a comprehensive understanding of the potential impact." In addition, some users and companies are now reporting that some of the patches offered to address the vulnerabilities are themselves creating new problems, such as freezing patched computers or interfering with anti-virus products. As nearly all modern technology companies are impacted by these vulnerabilities, and less than ten companies were included in the original June 2017 disclosure, it is reasonable to assume that additional companies have been negatively impacted by the embargo.

While we acknowledge that critical vulnerabilities such as these create challenging trade-offs between disclosure and secrecy, as premature disclosure may give malicious actors time to

---

3 Id.
4 See supra note 1.
5 See supra note 2.
exploit the vulnerabilities before mitigations are developed and deployed, we believe that this situation has shown the need for additional scrutiny regarding multi-party coordinated vulnerability disclosures. As demonstrated by numerous incidents over the past several years, cybersecurity is a collective responsibility. Further, it is a responsibility that is no longer limited solely to the information technology sector; connected products exist in electric grids, hospitals, manufacturing equipment, and in innumerable other sectors.

As more products and services become connected, no one company, or even one sector, working in isolation can provide sufficient protection for their products and users. Today, effective responses require extensive collaboration not only between individual companies, but also across sectors traditionally siloed from one another. This reality raises serious questions about not just the embargo imposed on information regarding the Meltdown and Spectre vulnerabilities, but on embargos regarding cybersecurity vulnerabilities in general.

Therefore, and pursuant to Rules X and XI of the United States House of Representatives, we ask that you respond to the following questions as soon as possible, but by no later than February 7, 2018:

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

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

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

4. When was the Computer Emergency Readiness Team Coordination Center (CERT/CC) 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 were the results?
   b. If no, why not?

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

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

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?

Please also arrange to provide a briefing on these issues to Committee staff by February 7, 2018. We appreciate your assistance with this request. If you should have any questions, please contact Jessica Wilkerson or John Ohly of the Majority Committee staff at (202) 225-2927.

Sincerely,

Greg Walden
Chairman

Maeha Blackburn
Chairman
Subcommittee on Communications and Technology

Robert E. Latta
Chairman
Subcommittee on Digital Commerce and Consumer Protection

Gregg Harper
Chairman
Subcommittee on Oversight and Investigations