

United States Senate

WASHINGTON, DC 20510

March 25, 2026

Mr. Sam Altman
Chief Executive Officer
OpenAI Foundation
1455 3rd Street
San Francisco, CA

Dear Mr. Altman:

As some of Congress's most vocal proponents for the modernization of national security missions with transformative technology, we have actively sought to ensure that the Department of Defense and Intelligence Community are equipped with capabilities drawn from the nation's leading innovators. These mission users – whose work has been guided by longstanding norms, legal procedures, and accountability mechanisms – benefit greatly from close collaboration with America's leading AI and advanced compute providers.

Correspondingly, American companies generate enduring public trust when Americans associate their products with efforts that enhance national security in effective, ethical, and lawful ways. At the same time – particularly against the backdrop of numerous pressures on those longstanding norms, procedures, and accountability mechanisms – it is imperative to anticipate potential failure modes for transformational technologies like AI, whether stemming from intentional misuse or insufficient oversight.

Recent developments concerning the Department of Defense's approach to AI suggest a troubling disregard for the kinds of safeguards in place to ensure that AI is being adopted with robust accountability. For instance, while foundational documents – such as the National Institute of Standards and Technology's *Artificial Intelligence Risk Management Framework*, the Office of Management and Budget's *Memorandum on Accelerating Federal Use of AI through Innovation, Governance, and Public Trust*, and the Final Report of the National Security Commission on Artificial Intelligence – underscore the central role of governance in effective AI utilization, the Department of Defense's January 9th *Artificial Intelligence Strategy for the Department of War* [sic] is conspicuously silent on this fundamental mission-enabler. While the *Strategy*'s emphasis on rapid adoption of commercial capabilities represents a legitimate objective, its clear disregard for mechanisms to ensure proper legal oversight (as well as meaningful test, evaluation, and validation technical safeguards) undermines U.S. security and American values.

A recent highly-publicized dispute between the Department and a leading American AI firm further suggests that this inattention towards – or even deliberate flouting of – AI governance may represent a systemic problem. Specifically, the Department recently rejected an existing vendor's request to memorialize a restriction on the use of its models for fully autonomous weapons or to facilitate bulk surveillance of Americans. These concerns are not unreasonable: against the recent backdrop of DoD lethal activity in Latin America – with the routine sidelining of military attorneys and the subversion of

longstanding norms on the use of lethal force – the Department’s aggressive insistence of an “any lawful use” standard provides unacceptable reputational risk and legal uncertainty for American companies.¹

Equally concerning, Defense Secretary Hegseth has taken an extraordinary and unprecedented step to designate a leading American tech company as a supply-chain risk to national security, with the ostensible intent of intimidating those prospective and existing government commercial and academic partners who might seek to ensure adequate safeguards for AI in military operations.² An American company fulfilling its contractual duties to the Department of Defense, while exercising its prerogative to ensure its products are lawfully, ethically, and appropriately used by the Department of Defense, is not a risk to national security or to America’s supply chain.³ While the ultimate responsibility for establishing robust and binding mechanisms to ensure lawful, appropriate, and effective AI rests with Congress, in the interim it is reasonable for commercial providers to ensure that products with outsized impact are governed with appropriate compliance mechanisms. Ultimately, strong AI governance for military and intelligence activity ensures the safety of servicemembers, the nation, and our allies and partners, while promoting clear and predictable norms in the face of less scrupulous adversaries.

Furthermore, the unprecedented designation of an American company, especially under such a weak policy and legal rationale, as a risk to the national security of the United States creates uncertainty among our allies and partners. Many of these countries are looking to incorporate American technology into their own national security and other government functions, and the specter of the Secretary utilizing a very serious sanction against more American companies, seemingly out of a sense of pique, will harm American companies in these global markets.

Your company has reportedly agreed in principle to have your AI model deployed for military purposes or to facilitate such deployment, subject to an “any lawful use” standard⁴ Accordingly, we respectfully request your response to the following questions by April 3, 2026:

1. Which specific models has your company made available to the Department of Defense, including Combat Support Agencies? Please specify the computing environments, and associated classification levels (via classified courier, if necessary).
2. Have the models made available to the Department of Defense been **trained or tested to deploy lethal autonomous warfare without human oversight or to conduct bulk surveillance of Americans**? If so, please specify the training or testing that was conducted, and provide the results of any such training or testing.
3. Does provision of your product include a contractual requirement for a **human on the loop** for autonomous kinetic operations? If not, please provide a clear rationale.

¹ How the Anthropic-Pentagon dispute over AI safeguards escalated. Reuters. (Mar. 11, 2026) <https://www.reuters.com/world/how-anthropic-pentagon-dispute-over-ai-safeguards-escalated-2026-03-11/>

² *Id.*

³ Per 10 USC 3252(d)(4), a supply chain risk is a designation reserved for adversaries who may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a covered system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system.

⁴

4. Does provision of your product include any specific, legally enforceable protections ensuring your AI model is **not used to conduct bulk surveillance on Americans in violation of the law**? If so, please specify which laws these provisions explicitly reference. If not, please provide a clear rationale.
5. What additional forms of AI governance – including documentation, testing and validation, auditability, and performance monitoring – do you ensure through contractual or technical controls for products used in high-impact national security contexts?
6. Under what circumstances would your company acquiesce to any unlawful uses of its product by the Department of Defense?
7. To the extent that your contract permits appropriately cleared Forward Deployed Engineers, does your company have internal company reporting mechanisms or procedures to enable cleared staff to alert uncleared corporate leadership of potential misuse? Provide documentation sufficient to substantiate any such asserted mechanisms or procedures.
8. Under what circumstances would your company inform appropriate Congressional Committees of unlawful or unethical use of your products by the Department of Defense? If there is a contractual limitation on notifying Congress, please indicate such a mechanism and provide documentation sufficient to substantiate that limitation.
9. Does your model Usage Policy provide you with special capabilities to control, oversee, second-guess, impede, or intervene in the Department of Defense’s military judgments, decision-making, or operations?

Thank you for your attention to this matter.

Sincerely,



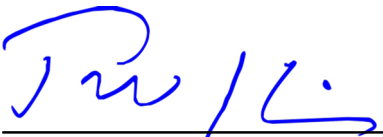
Mark R. Warner
United States Senator



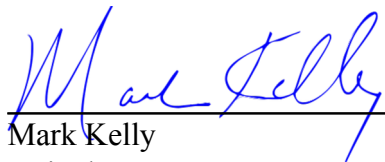
Christopher A. Coons
United States Senator



Kirsten Gillibrand
United States Senator



Tim Kaine
United States Senator



Mark Kelly
United States Senator



Elissa Slotkin
United States Senator

United States Senate

WASHINGTON, DC 20510

March 25, 2026

Mr. Matt Garman
Chief Executive Officer
Amazon Web Services, Inc.
410 Terry Ave N
Seattle, WA 98109

Dear Mr. Garman:

As some of Congress's most vocal proponents for the modernization of national security missions with transformative technology, we have actively sought to ensure that the Department of Defense and Intelligence Community are equipped with capabilities drawn from the nation's leading innovators. These mission users – whose work has been guided by longstanding norms, legal procedures, and accountability mechanisms – benefit greatly from close collaboration with America's leading AI and advanced compute providers.

Correspondingly, American companies generate enduring public trust when Americans associate their products with efforts that enhance national security in effective, ethical, and lawful ways. At the same time – particularly against the backdrop of numerous pressures on those longstanding norms, procedures, and accountability mechanisms – it is imperative to anticipate potential failure modes for transformational technologies like AI, whether stemming from intentional misuse or insufficient oversight.

Recent developments concerning the Department of Defense's approach to AI suggest a troubling disregard for the kinds of safeguards in place to ensure that AI is being adopted with robust accountability. For instance, while foundational documents – such as the National Institute of Standards and Technology's *Artificial Intelligence Risk Management Framework*, the Office of Management and Budget's *Memorandum on Accelerating Federal Use of AI through Innovation, Governance, and Public Trust*, and the Final Report of the National Security Commission on Artificial Intelligence – underscore the central role of governance in effective AI utilization, the Department of Defense's January 9th *Artificial Intelligence Strategy for the Department of War* [sic] is conspicuously silent on this fundamental mission-enabler. While the *Strategy*'s emphasis on rapid adoption of commercial capabilities represents a legitimate objective, its clear disregard for mechanisms to ensure proper legal oversight (as well as meaningful test, evaluation, and validation technical safeguards) undermines U.S. security and American values.

A recent highly-publicized dispute between the Department and a leading American AI firm further suggests that this inattention towards – or even deliberate flouting of – AI governance may represent a systemic problem. Specifically, the Department recently rejected an existing vendor's request to memorialize a restriction on the use of its models for fully autonomous weapons or to facilitate bulk surveillance of Americans. These concerns are not unreasonable: against the recent backdrop of DoD lethal activity in Latin America – with the routine sidelining of military attorneys and the subversion of

longstanding norms on the use of lethal force – the Department’s aggressive insistence of an “any lawful use” standard provides unacceptable reputational risk and legal uncertainty for American companies.¹

Equally concerning, Defense Secretary Hegseth has taken an extraordinary and unprecedented step to designate a leading American tech company as a supply-chain risk to national security, with the ostensible intent of intimidating those prospective and existing government commercial and academic partners who might seek to ensure adequate safeguards for AI in military operations.² An American company fulfilling its contractual duties to the Department of Defense, while exercising its prerogative to ensure its products are lawfully, ethically, and appropriately used by the Department of Defense, is not a risk to national security or to America’s supply chain.³ While the ultimate responsibility for establishing robust and binding mechanisms to ensure lawful, appropriate, and effective AI rests with Congress, in the interim it is reasonable for commercial providers to ensure that products with outsized impact are governed with appropriate compliance mechanisms. Ultimately, strong AI governance for military and intelligence activity ensures the safety of servicemembers, the nation, and our allies and partners, while promoting clear and predictable norms in the face of less scrupulous adversaries.

Furthermore, the unprecedented designation of an American company, especially under such a weak policy and legal rationale, as a risk to the national security of the United States creates uncertainty among our allies and partners. Many of these countries are looking to incorporate American technology into their own national security and other government functions, and the specter of the Secretary utilizing a very serious sanction against more American companies, seemingly out of a sense of pique, will harm American companies in these global markets.

Your company has reportedly agreed in principle to have your AI model deployed for military purposes or to facilitate such deployment, subject to an “any lawful use” standard⁴ Accordingly, we respectfully request your response to the following questions by April 3, 2026:

1. Which specific models has your company made available to the Department of Defense, including Combat Support Agencies? Please specify the computing environments, and associated classification levels (via classified courier, if necessary).
2. Have the models made available to the Department of Defense been **trained or tested to deploy lethal autonomous warfare without human oversight or to conduct bulk surveillance of Americans**? If so, please specify the training or testing that was conducted, and provide the results of any such training or testing.
3. Does provision of your product include a contractual requirement for a **human on the loop** for autonomous kinetic operations? If not, please provide a clear rationale.

¹ How the Anthropic-Pentagon dispute over AI safeguards escalated. Reuters. (Mar. 11, 2026) <https://www.reuters.com/world/how-anthropic-pentagon-dispute-over-ai-safeguards-escalated-2026-03-11/>

²*Id.*

³ Per 10 USC 3252(d)(4), a supply chain risk is a designation reserved for adversaries who may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a covered system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system.

⁴

4. Does provision of your product include any specific, legally enforceable protections ensuring your AI model is **not used to conduct bulk surveillance on Americans in violation of the law**? If so, please specify which laws these provisions explicitly reference. If not, please provide a clear rationale.
5. What additional forms of AI governance – including documentation, testing and validation, auditability, and performance monitoring – do you ensure through contractual or technical controls for products used in high-impact national security contexts?
6. Under what circumstances would your company acquiesce to any unlawful uses of its product by the Department of Defense?
7. To the extent that your contract permits appropriately cleared Forward Deployed Engineers, does your company have internal company reporting mechanisms or procedures to enable cleared staff to alert uncleared corporate leadership of potential misuse? Provide documentation sufficient to substantiate any such asserted mechanisms or procedures.
8. Under what circumstances would your company inform appropriate Congressional Committees of unlawful or unethical use of your products by the Department of Defense? If there is a contractual limitation on notifying Congress, please indicate such a mechanism and provide documentation sufficient to substantiate that limitation.
9. Does your model Usage Policy provide you with special capabilities to control, oversee, second-guess, impede, or intervene in the Department of Defense’s military judgments, decision-making, or operations?

Thank you for your attention to this matter.

Sincerely,



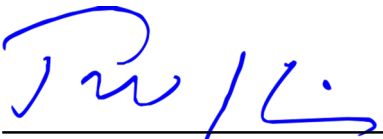
Mark R. Warner
United States Senator



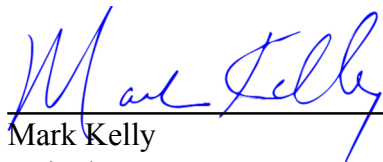
Christopher A. Coons
United States Senator



Kirsten Gillibrand
United States Senator



Tim Kaine
United States Senator



Mark Kelly
United States Senator



Elissa Slotkin
United States Senator

United States Senate

WASHINGTON, DC 20510

March 25, 2026

Mr. Elon Musk
Chief Executive Officer
xAI Corp.
1450 Page Mill Road
Palo Alto, CA 94304

Dear Mr. Musk:

As some of Congress's most vocal proponents for the modernization of national security missions with transformative technology, we have actively sought to ensure that the Department of Defense and Intelligence Community are equipped with capabilities drawn from the nation's leading innovators. These mission users – whose work has been guided by longstanding norms, legal procedures, and accountability mechanisms – benefit greatly from close collaboration with America's leading AI and advanced compute providers.

Correspondingly, American companies generate enduring public trust when Americans associate their products with efforts that enhance national security in effective, ethical, and lawful ways. At the same time – particularly against the backdrop of numerous pressures on those longstanding norms, procedures, and accountability mechanisms – it is imperative to anticipate potential failure modes for transformational technologies like AI, whether stemming from intentional misuse or insufficient oversight.

Recent developments concerning the Department of Defense's approach to AI suggest a troubling disregard for the kinds of safeguards in place to ensure that AI is being adopted with robust accountability. For instance, while foundational documents – such as the National Institute of Standards and Technology's *Artificial Intelligence Risk Management Framework*, the Office of Management and Budget's *Memorandum on Accelerating Federal Use of AI through Innovation, Governance, and Public Trust*, and the Final Report of the National Security Commission on Artificial Intelligence – underscore the central role of governance in effective AI utilization, the Department of Defense's January 9th *Artificial Intelligence Strategy for the Department of War* [sic] is conspicuously silent on this fundamental mission-enabler. While the *Strategy*'s emphasis on rapid adoption of commercial capabilities represents a legitimate objective, its clear disregard for mechanisms to ensure proper legal oversight (as well as meaningful test, evaluation, and validation technical safeguards) undermines U.S. security and American values.

A recent highly-publicized dispute between the Department and a leading American AI firm further suggests that this inattention towards – or even deliberate flouting of – AI governance may represent a systemic problem. Specifically, the Department recently rejected an existing vendor's request to memorialize a restriction on the use of its models for fully autonomous weapons or to facilitate bulk surveillance of Americans. These concerns are not unreasonable: against the recent backdrop of DoD lethal activity in Latin America – with the routine sidelining of military attorneys and the subversion of

longstanding norms on the use of lethal force – the Department’s aggressive insistence of an “any lawful use” standard provides unacceptable reputational risk and legal uncertainty for American companies.¹

Equally concerning, Defense Secretary Hegseth has taken an extraordinary and unprecedented step to designate a leading American tech company as a supply-chain risk to national security, with the ostensible intent of intimidating those prospective and existing government commercial and academic partners who might seek to ensure adequate safeguards for AI in military operations.² An American company fulfilling its contractual duties to the Department of Defense, while exercising its prerogative to ensure its products are lawfully, ethically, and appropriately used by the Department of Defense, is not a risk to national security or to America’s supply chain.³ While the ultimate responsibility for establishing robust and binding mechanisms to ensure lawful, appropriate, and effective AI rests with Congress, in the interim it is reasonable for commercial providers to ensure that products with outsized impact are governed with appropriate compliance mechanisms. Ultimately, strong AI governance for military and intelligence activity ensures the safety of servicemembers, the nation, and our allies and partners, while promoting clear and predictable norms in the face of less scrupulous adversaries.

Furthermore, the unprecedented designation of an American company, especially under such a weak policy and legal rationale, as a risk to the national security of the United States creates uncertainty among our allies and partners. Many of these countries are looking to incorporate American technology into their own national security and other government functions, and the specter of the Secretary utilizing a very serious sanction against more American companies, seemingly out of a sense of pique, will harm American companies in these global markets.

Your company has reportedly agreed in principle to have your AI model deployed for military purposes or to facilitate such deployment, subject to an “any lawful use” standard⁴ Accordingly, we respectfully request your response to the following questions by April 3, 2026:

1. Which specific models has your company made available to the Department of Defense, including Combat Support Agencies? Please specify the computing environments, and associated classification levels (via classified courier, if necessary).
2. Have the models made available to the Department of Defense been **trained or tested to deploy lethal autonomous warfare without human oversight or to conduct bulk surveillance of Americans**? If so, please specify the training or testing that was conducted, and provide the results of any such training or testing.
3. Does provision of your product include a contractual requirement for a **human on the loop** for autonomous kinetic operations? If not, please provide a clear rationale.

¹ How the Anthropic-Pentagon dispute over AI safeguards escalated. Reuters. (Mar. 11, 2026) <https://www.reuters.com/world/how-anthropic-pentagon-dispute-over-ai-safeguards-escalated-2026-03-11/>

²*Id.*

³ Per 10 USC 3252(d)(4), a supply chain risk is a designation reserved for adversaries who may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a covered system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system.

⁴

4. Does provision of your product include any specific, legally enforceable protections ensuring your AI model is **not used to conduct bulk surveillance on Americans in violation of the law**? If so, please specify which laws these provisions explicitly reference. If not, please provide a clear rationale.
5. What additional forms of AI governance – including documentation, testing and validation, auditability, and performance monitoring – do you ensure through contractual or technical controls for products used in high-impact national security contexts?
6. Under what circumstances would your company acquiesce to any unlawful uses of its product by the Department of Defense?
7. To the extent that your contract permits appropriately cleared Forward Deployed Engineers, does your company have internal company reporting mechanisms or procedures to enable cleared staff to alert uncleared corporate leadership of potential misuse? Provide documentation sufficient to substantiate any such asserted mechanisms or procedures.
8. Under what circumstances would your company inform appropriate Congressional Committees of unlawful or unethical use of your products by the Department of Defense? If there is a contractual limitation on notifying Congress, please indicate such a mechanism and provide documentation sufficient to substantiate that limitation.
9. Does your model Usage Policy provide you with special capabilities to control, oversee, second-guess, impede, or intervene in the Department of Defense’s military judgments, decision-making, or operations?

Thank you for your attention to this matter.

Sincerely,



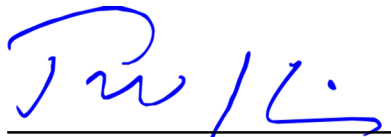
Mark R. Warner
United States Senator



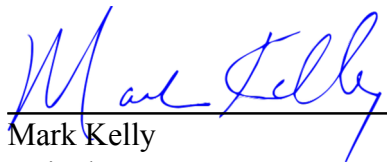
Christopher A. Coons
United States Senator



Kirsten Gillibrand
United States Senator



Tim Kaine
United States Senator



Mark Kelly
United States Senator



Elissa Slotkin
United States Senator

United States Senate

WASHINGTON, DC 20510

March 25, 2026

Mr. Sundar Pichai
Chief Executive Officer
Alphabet, Inc.
1600 Amphitheatre Parkway
Mountain View, CA 94043

Dear Mr. Pichai:

As some of Congress's most vocal proponents for the modernization of national security missions with transformative technology, we have actively sought to ensure that the Department of Defense and Intelligence Community are equipped with capabilities drawn from the nation's leading innovators. These mission users – whose work has been guided by longstanding norms, legal procedures, and accountability mechanisms – benefit greatly from close collaboration with America's leading AI and advanced compute providers.

Correspondingly, American companies generate enduring public trust when Americans associate their products with efforts that enhance national security in effective, ethical, and lawful ways. At the same time – particularly against the backdrop of numerous pressures on those longstanding norms, procedures, and accountability mechanisms – it is imperative to anticipate potential failure modes for transformational technologies like AI, whether stemming from intentional misuse or insufficient oversight.

Recent developments concerning the Department of Defense's approach to AI suggest a troubling disregard for the kinds of safeguards in place to ensure that AI is being adopted with robust accountability. For instance, while foundational documents – such as the National Institute of Standards and Technology's *Artificial Intelligence Risk Management Framework*, the Office of Management and Budget's *Memorandum on Accelerating Federal Use of AI through Innovation, Governance, and Public Trust*, and the Final Report of the National Security Commission on Artificial Intelligence – underscore the central role of governance in effective AI utilization, the Department of Defense's January 9th *Artificial Intelligence Strategy for the Department of War* [sic] is conspicuously silent on this fundamental mission-enabler. While the *Strategy*'s emphasis on rapid adoption of commercial capabilities represents a legitimate objective, its clear disregard for mechanisms to ensure proper legal oversight (as well as meaningful test, evaluation, and validation technical safeguards) undermines U.S. security and American values.

A recent highly-publicized dispute between the Department and a leading American AI firm further suggests that this inattention towards – or even deliberate flouting of – AI governance may represent a systemic problem. Specifically, the Department recently rejected an existing vendor's request to memorialize a restriction on the use of its models for fully autonomous weapons or to facilitate bulk surveillance of Americans. These concerns are not unreasonable: against the recent backdrop of DoD lethal activity in Latin America – with the routine sidelining of military attorneys and the subversion of

longstanding norms on the use of lethal force – the Department’s aggressive insistence of an “any lawful use” standard provides unacceptable reputational risk and legal uncertainty for American companies.¹

Equally concerning, Defense Secretary Hegseth has taken an extraordinary and unprecedented step to designate a leading American tech company as a supply-chain risk to national security, with the ostensible intent of intimidating those prospective and existing government commercial and academic partners who might seek to ensure adequate safeguards for AI in military operations.² An American company fulfilling its contractual duties to the Department of Defense, while exercising its prerogative to ensure its products are lawfully, ethically, and appropriately used by the Department of Defense, is not a risk to national security or to America’s supply chain.³ While the ultimate responsibility for establishing robust and binding mechanisms to ensure lawful, appropriate, and effective AI rests with Congress, in the interim it is reasonable for commercial providers to ensure that products with outsized impact are governed with appropriate compliance mechanisms. Ultimately, strong AI governance for military and intelligence activity ensures the safety of servicemembers, the nation, and our allies and partners, while promoting clear and predictable norms in the face of less scrupulous adversaries.

Furthermore, the unprecedented designation of an American company, especially under such a weak policy and legal rationale, as a risk to the national security of the United States creates uncertainty among our allies and partners. Many of these countries are looking to incorporate American technology into their own national security and other government functions, and the specter of the Secretary utilizing a very serious sanction against more American companies, seemingly out of a sense of pique, will harm American companies in these global markets.

Your company has reportedly agreed in principle to have your AI model deployed for military purposes or to facilitate such deployment, subject to an “any lawful use” standard⁴ Accordingly, we respectfully request your response to the following questions by April 3, 2026:

1. Which specific models has your company made available to the Department of Defense, including Combat Support Agencies? Please specify the computing environments, and associated classification levels (via classified courier, if necessary).
2. Have the models made available to the Department of Defense been **trained or tested to deploy lethal autonomous warfare without human oversight or to conduct bulk surveillance of Americans**? If so, please specify the training or testing that was conducted, and provide the results of any such training or testing.
3. Does provision of your product include a contractual requirement for a **human on the loop** for autonomous kinetic operations? If not, please provide a clear rationale.

¹ How the Anthropic-Pentagon dispute over AI safeguards escalated. Reuters. (Mar. 11, 2026) <https://www.reuters.com/world/how-anthropic-pentagon-dispute-over-ai-safeguards-escalated-2026-03-11/>

²*Id.*

³ Per 10 USC 3252(d)(4), a supply chain risk is a designation reserved for adversaries who may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a covered system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system.

⁴

4. Does provision of your product include any specific, legally enforceable protections ensuring your AI model is **not used to conduct bulk surveillance on Americans in violation of the law**? If so, please specify which laws these provisions explicitly reference. If not, please provide a clear rationale.
5. What additional forms of AI governance – including documentation, testing and validation, auditability, and performance monitoring – do you ensure through contractual or technical controls for products used in high-impact national security contexts?
6. Under what circumstances would your company acquiesce to any unlawful uses of its product by the Department of Defense?
7. To the extent that your contract permits appropriately cleared Forward Deployed Engineers, does your company have internal company reporting mechanisms or procedures to enable cleared staff to alert uncleared corporate leadership of potential misuse? Provide documentation sufficient to substantiate any such asserted mechanisms or procedures.
8. Under what circumstances would your company inform appropriate Congressional Committees of unlawful or unethical use of your products by the Department of Defense? If there is a contractual limitation on notifying Congress, please indicate such a mechanism and provide documentation sufficient to substantiate that limitation.
9. Does your model Usage Policy provide you with special capabilities to control, oversee, second-guess, impede, or intervene in the Department of Defense’s military judgments, decision-making, or operations?

Thank you for your attention to this matter.

Sincerely,



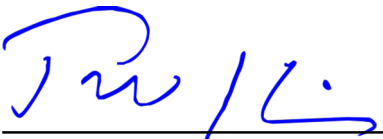
Mark R. Warner
United States Senator



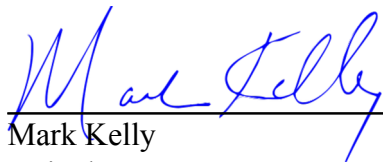
Christopher A. Coons
United States Senator



Kirsten Gillibrand
United States Senator



Tim Kaine
United States Senator



Mark Kelly
United States Senator



Elissa Slotkin
United States Senator

United States Senate

WASHINGTON, DC 20510

March 25, 2026

Mr. Mustafa Suleyman
Chief Executive Officer
Microsoft AI
Building 99, 14820 NE 36th Street
Redmond, Washington

Dear Mr. Suleyman:

As some of Congress's most vocal proponents for the modernization of national security missions with transformative technology, we have actively sought to ensure that the Department of Defense and Intelligence Community are equipped with capabilities drawn from the nation's leading innovators. These mission users – whose work has been guided by longstanding norms, legal procedures, and accountability mechanisms – benefit greatly from close collaboration with America's leading AI and advanced compute providers.

Correspondingly, American companies generate enduring public trust when Americans associate their products with efforts that enhance national security in effective, ethical, and lawful ways. At the same time – particularly against the backdrop of numerous pressures on those longstanding norms, procedures, and accountability mechanisms – it is imperative to anticipate potential failure modes for transformational technologies like AI, whether stemming from intentional misuse or insufficient oversight.

Recent developments concerning the Department of Defense's approach to AI suggest a troubling disregard for the kinds of safeguards in place to ensure that AI is being adopted with robust accountability. For instance, while foundational documents – such as the National Institute of Standards and Technology's *Artificial Intelligence Risk Management Framework*, the Office of Management and Budget's *Memorandum on Accelerating Federal Use of AI through Innovation, Governance, and Public Trust*, and the Final Report of the National Security Commission on Artificial Intelligence – underscore the central role of governance in effective AI utilization, the Department of Defense's January 9th *Artificial Intelligence Strategy for the Department of War* [sic] is conspicuously silent on this fundamental mission-enabler. While the *Strategy*'s emphasis on rapid adoption of commercial capabilities represents a legitimate objective, its clear disregard for mechanisms to ensure proper legal oversight (as well as meaningful test, evaluation, and validation technical safeguards) undermines U.S. security and American values.

A recent highly-publicized dispute between the Department and a leading American AI firm further suggests that this inattention towards – or even deliberate flouting of – AI governance may represent a systemic problem. Specifically, the Department recently rejected an existing vendor's request to memorialize a restriction on the use of its models for fully autonomous weapons or to facilitate bulk surveillance of Americans. These concerns are not unreasonable: against the recent backdrop of DoD lethal activity in Latin America – with the routine sidelining of military attorneys and the subversion of

longstanding norms on the use of lethal force – the Department’s aggressive insistence of an “any lawful use” standard provides unacceptable reputational risk and legal uncertainty for American companies.¹

Equally concerning, Defense Secretary Hegseth has taken an extraordinary and unprecedented step to designate a leading American tech company as a supply-chain risk to national security, with the ostensible intent of intimidating those prospective and existing government commercial and academic partners who might seek to ensure adequate safeguards for AI in military operations.² An American company fulfilling its contractual duties to the Department of Defense, while exercising its prerogative to ensure its products are lawfully, ethically, and appropriately used by the Department of Defense, is not a risk to national security or to America’s supply chain.³ While the ultimate responsibility for establishing robust and binding mechanisms to ensure lawful, appropriate, and effective AI rests with Congress, in the interim it is reasonable for commercial providers to ensure that products with outsized impact are governed with appropriate compliance mechanisms. Ultimately, strong AI governance for military and intelligence activity ensures the safety of servicemembers, the nation, and our allies and partners, while promoting clear and predictable norms in the face of less scrupulous adversaries.

Furthermore, the unprecedented designation of an American company, especially under such a weak policy and legal rationale, as a risk to the national security of the United States creates uncertainty among our allies and partners. Many of these countries are looking to incorporate American technology into their own national security and other government functions, and the specter of the Secretary utilizing a very serious sanction against more American companies, seemingly out of a sense of pique, will harm American companies in these global markets.

Your company has reportedly agreed in principle to have your AI model deployed for military purposes or to facilitate such deployment, subject to an “any lawful use” standard⁴ Accordingly, we respectfully request your response to the following questions by April 3, 2026:

1. Which specific models has your company made available to the Department of Defense, including Combat Support Agencies? Please specify the computing environments, and associated classification levels (via classified courier, if necessary).
2. Have the models made available to the Department of Defense been **trained or tested to deploy lethal autonomous warfare without human oversight or to conduct bulk surveillance of Americans**? If so, please specify the training or testing that was conducted, and provide the results of any such training or testing.
3. Does provision of your product include a contractual requirement for a **human on the loop** for autonomous kinetic operations? If not, please provide a clear rationale.

¹ How the Anthropic-Pentagon dispute over AI safeguards escalated. Reuters. (Mar. 11, 2026) <https://www.reuters.com/world/how-anthropic-pentagon-dispute-over-ai-safeguards-escalated-2026-03-11/>

²*Id.*

³ Per 10 USC 3252(d)(4), a supply chain risk is a designation reserved for adversaries who may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a covered system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system.

⁴

4. Does provision of your product include any specific, legally enforceable protections ensuring your AI model is **not used to conduct bulk surveillance on Americans in violation of the law**? If so, please specify which laws these provisions explicitly reference. If not, please provide a clear rationale.
5. What additional forms of AI governance – including documentation, testing and validation, auditability, and performance monitoring – do you ensure through contractual or technical controls for products used in high-impact national security contexts?
6. Under what circumstances would your company acquiesce to any unlawful uses of its product by the Department of Defense?
7. To the extent that your contract permits appropriately cleared Forward Deployed Engineers, does your company have internal company reporting mechanisms or procedures to enable cleared staff to alert uncleared corporate leadership of potential misuse? Provide documentation sufficient to substantiate any such asserted mechanisms or procedures.
8. Under what circumstances would your company inform appropriate Congressional Committees of unlawful or unethical use of your products by the Department of Defense? If there is a contractual limitation on notifying Congress, please indicate such a mechanism and provide documentation sufficient to substantiate that limitation.
9. Does your model Usage Policy provide you with special capabilities to control, oversee, second-guess, impede, or intervene in the Department of Defense’s military judgments, decision-making, or operations?

Thank you for your attention to this matter.

Sincerely,



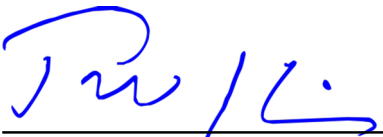
Mark R. Warner
United States Senator



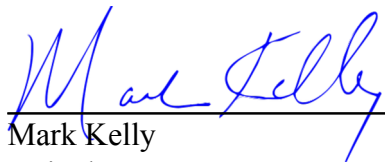
Christopher A. Coons
United States Senator



Kirsten Gillibrand
United States Senator



Tim Kaine
United States Senator



Mark Kelly
United States Senator



Elissa Slotkin
United States Senator

United States Senate

WASHINGTON, DC 20510

March 25, 2026

Mr. Mark Zuckerberg
Chief Executive Officer
Meta, Inc.
1 Meta Way
Menlo Park, CA 94025

Dear Mr. Zuckerberg:

As some of Congress's most vocal proponents for the modernization of national security missions with transformative technology, we have actively sought to ensure that the Department of Defense and Intelligence Community are equipped with capabilities drawn from the nation's leading innovators. These mission users – whose work has been guided by longstanding norms, legal procedures, and accountability mechanisms – benefit greatly from close collaboration with America's leading AI and advanced compute providers.

Correspondingly, American companies generate enduring public trust when Americans associate their products with efforts that enhance national security in effective, ethical, and lawful ways. At the same time – particularly against the backdrop of numerous pressures on those longstanding norms, procedures, and accountability mechanisms – it is imperative to anticipate potential failure modes for transformational technologies like AI, whether stemming from intentional misuse or insufficient oversight.

Recent developments concerning the Department of Defense's approach to AI suggest a troubling disregard for the kinds of safeguards in place to ensure that AI is being adopted with robust accountability. For instance, while foundational documents – such as the National Institute of Standards and Technology's *Artificial Intelligence Risk Management Framework*, the Office of Management and Budget's *Memorandum on Accelerating Federal Use of AI through Innovation, Governance, and Public Trust*, and the Final Report of the National Security Commission on Artificial Intelligence – underscore the central role of governance in effective AI utilization, the Department of Defense's January 9th *Artificial Intelligence Strategy for the Department of War* [sic] is conspicuously silent on this fundamental mission-enabler. While the *Strategy*'s emphasis on rapid adoption of commercial capabilities represents a legitimate objective, its clear disregard for mechanisms to ensure proper legal oversight (as well as meaningful test, evaluation, and validation technical safeguards) undermines U.S. security and American values.

A recent highly-publicized dispute between the Department and a leading American AI firm further suggests that this inattention towards – or even deliberate flouting of – AI governance may represent a systemic problem. Specifically, the Department recently rejected an existing vendor's request to memorialize a restriction on the use of its models for fully autonomous weapons or to facilitate bulk surveillance of Americans. These concerns are not unreasonable: against the recent backdrop of DoD lethal activity in Latin America – with the routine sidelining of military attorneys and the subversion of

longstanding norms on the use of lethal force – the Department’s aggressive insistence of an “any lawful use” standard provides unacceptable reputational risk and legal uncertainty for American companies.¹

Equally concerning, Defense Secretary Hegseth has taken an extraordinary and unprecedented step to designate a leading American tech company as a supply-chain risk to national security, with the ostensible intent of intimidating those prospective and existing government commercial and academic partners who might seek to ensure adequate safeguards for AI in military operations.² An American company fulfilling its contractual duties to the Department of Defense, while exercising its prerogative to ensure its products are lawfully, ethically, and appropriately used by the Department of Defense, is not a risk to national security or to America’s supply chain.³ While the ultimate responsibility for establishing robust and binding mechanisms to ensure lawful, appropriate, and effective AI rests with Congress, in the interim it is reasonable for commercial providers to ensure that products with outsized impact are governed with appropriate compliance mechanisms. Ultimately, strong AI governance for military and intelligence activity ensures the safety of servicemembers, the nation, and our allies and partners, while promoting clear and predictable norms in the face of less scrupulous adversaries.

Furthermore, the unprecedented designation of an American company, especially under such a weak policy and legal rationale, as a risk to the national security of the United States creates uncertainty among our allies and partners. Many of these countries are looking to incorporate American technology into their own national security and other government functions, and the specter of the Secretary utilizing a very serious sanction against more American companies, seemingly out of a sense of pique, will harm American companies in these global markets.

Your company has reportedly agreed in principle to have your AI model deployed for military purposes or to facilitate such deployment, subject to an “any lawful use” standard⁴ Accordingly, we respectfully request your response to the following questions by April 3, 2026:

1. Which specific models has your company made available to the Department of Defense, including Combat Support Agencies? Please specify the computing environments, and associated classification levels (via classified courier, if necessary).
2. Have the models made available to the Department of Defense been **trained or tested to deploy lethal autonomous warfare without human oversight or to conduct bulk surveillance of Americans**? If so, please specify the training or testing that was conducted, and provide the results of any such training or testing.
3. Does provision of your product include a contractual requirement for a **human on the loop** for autonomous kinetic operations? If not, please provide a clear rationale.

¹ How the Anthropic-Pentagon dispute over AI safeguards escalated. Reuters. (Mar. 11, 2026) <https://www.reuters.com/world/how-anthropic-pentagon-dispute-over-ai-safeguards-escalated-2026-03-11/>

² *Id.*

³ Per 10 USC 3252(d)(4), a supply chain risk is a designation reserved for adversaries who may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a covered system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system.

⁴

4. Does provision of your product include any specific, legally enforceable protections ensuring your AI model is **not used to conduct bulk surveillance on Americans in violation of the law**? If so, please specify which laws these provisions explicitly reference. If not, please provide a clear rationale.
5. What additional forms of AI governance – including documentation, testing and validation, auditability, and performance monitoring – do you ensure through contractual or technical controls for products used in high-impact national security contexts?
6. Under what circumstances would your company acquiesce to any unlawful uses of its product by the Department of Defense?
7. To the extent that your contract permits appropriately cleared Forward Deployed Engineers, does your company have internal company reporting mechanisms or procedures to enable cleared staff to alert uncleared corporate leadership of potential misuse? Provide documentation sufficient to substantiate any such asserted mechanisms or procedures.
8. Under what circumstances would your company inform appropriate Congressional Committees of unlawful or unethical use of your products by the Department of Defense? If there is a contractual limitation on notifying Congress, please indicate such a mechanism and provide documentation sufficient to substantiate that limitation.
9. Does your model Usage Policy provide you with special capabilities to control, oversee, second-guess, impede, or intervene in the Department of Defense’s military judgments, decision-making, or operations?

Thank you for your attention to this matter.

Sincerely,



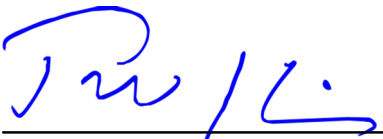
Mark R. Warner
United States Senator



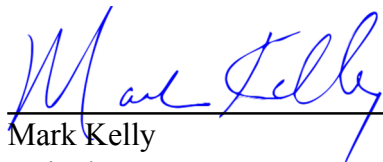
Christopher A. Coons
United States Senator



Kirsten Gillibrand
United States Senator



Tim Kaine
United States Senator



Mark Kelly
United States Senator



Elissa Slotkin
United States Senator