No. 26-1049

IN THE UNITED STATES COURT OF APPEALS
FOR THE DISTRICT OF COLUMBIA CIRCUIT

ANTHROPIC PBC,

Petitioner,

v.

U.S. DEPARTMENT OF WAR, et al.,

Respondents.

On Petition for Review of Agency Action

RESPONSE IN OPPOSITION TO EMERGENCY MOTION FOR STAY PENDING REVIEW

BRETT A. SHUMATE
Assistant Attorney General

SHARON SWINGLE
SEAN R. JANDA
BRIAN J. SPRINGER
Attorneys, Appellate Staff
Civil Division, Room 7260
U.S. Department of Justice
950 Pennsylvania Avenue NW
Washington, D.C. 20530
(202) 514-3388
sean.r.janda@usdoj.gov

TABLE OF CONTENTS

INTRODUCTION

Petitioner Anthropic PBC's artificial-intelligence software is integrated into the military's most sensitive systems, including its classified systems, and used in active military operations. Because of the nature of the technology, petitioner retains substantial control over the functioning of its software even while used by the military. The Secretary of War has recently determined, however, that petitioner's behavior has undermined the trust required to sustain that relationship and given rise to the risk that petitioner may unilaterally manipulate its software to enforce its own moral and policy judgments about the military's appropriate use of the software. As a result, the Secretary has determined that the continued integration of petitioner's software into the Department of War's systems presents an untenable national-security risk.

The effect of that determination is limited: it prohibits the Department from contracting with petitioner and prohibits Department contractors from using petitioner's software when working on Department contracts. It does not prohibit petitioner from contracting with other entities, including other federal agencies and Department contractors for work that does not involve Department contracts. It is, in other words, exactly the sort of limited

measure that petitioner's declarant states the Department may reasonably take if it does not believe that petitioner's product—with petitioner's imposed limitations—fits the Department's needs.

Nonetheless, petitioner now asks this Court to countermand the Secretary's considered national-security judgment—and to do so on an emergency basis without the benefit of full briefing. That request is meritless on all levels. Most importantly, the Secretary's determination of the national-security risks associated with the Department's continued use of petitioner's software is well supported by the record. Such predictive national-security assessments are best made by the political branches, and those risks prevent petitioner from demonstrating that emergency relief is warranted.

But even beyond that, petitioner's motion is unsound. The motion reflects a premature rush to the courthouse before the administrative process is complete and seeks interim relief not contemplated by the statute. And because petitioner filed its motion before receiving the Secretary's determination or supporting materials, the motion can do no more than speculate (often erroneously) about the procedural and substantive basis for

the Secretary's action. With the benefit of that record, it is clear that petitioner is unlikely to succeed on any of the various claims asserted.

Regardless, petitioner cannot demonstrate immediate irreparable injury attributable to the Secretary's determination or redressable by a stay. Petitioner has no right to contract with the Department—especially on terms that do not serve the Department's operational needs—and many of petitioner's asserted harms depend on speculation about third parties' reactions to the government's actions. By contrast, the government's and the public's interests counsel against requiring the Department to tolerate the risk that critical military systems will be jeopardized at pivotal moments.

The motion should be denied.

STATEMENT

1. The Federal Acquisition Supply Chain Security Act of 2018, Pub. L. No. 115-390, tit. II, 132 Stat. 5173, seeks to mitigate the risk that contractors may tamper with technologies incorporated in government systems. *See* S. Rep. No. 115-408, at 1-2 (2018). An agency head may deem a source to be a supply chain risk where "any person may sabotage, maliciously introduce unwanted function, extract data, or otherwise manipulate" the source's technology "so as to surveil, deny, disrupt, or otherwise manipulate" the use

of the technology or the "information stored or transmitted" thereon. 41 U.S.C. § 4713(k)(6). After making the requisite determinations, the agency may, among other things, "withhold consent for a contractor to subcontract with [the] particular source" and order "exclusion of [the] source." *Id.* § 4713(k)(4).

To exercise this authority, the agency head "obtain[s] a joint recommendation" from certain agency officials with an assessment "that there is a significant supply chain risk." 41 U.S.C. § 4713(b)(1). The agency head "mak[es] a determination in writing" that excluding the source "is necessary to protect national security by reducing supply chain risk" and that "less intrusive measures are not reasonably available to reduce" that risk. *Id.* § 4713(b)(3)(A)-(B). The resulting designation "specifies the scope of the determination," including the types of procurements covered. *Id.* § 4713(b)(3)(C). And the agency provides notice to certain congressional committees. *Id.* § 4713(b)(4).

Under the statute, the source also receives notice and an opportunity to respond. *See* 41 U.S.C. § 4713(b)(2). That process usually occurs before the designation, but Congress has authorized the agency head to delay notice until after the designation if he "determines that an urgent national security

interest requires" immediate action. *See id.* § 4713(c). In such a circumstance, the agency head must, "as soon as practicable after addressing the urgent national security interest," "provid[e] the notice" to the source, "consider[] any information submitted by the source," and "mak[e] any appropriate modifications to the determination based on such information." *Id.* § 4713(c)(2)(A)-(C).

2. Petitioner is a software company that has developed an AI model called Claude. Add.23. Since 2024, the government has employed petitioner's model for various uses, through both direct contracts with petitioner and integration of petitioner's software into products or services provided by other government contractors. *See* Add.48-50. Petitioner's software has been deployed by the Department for highly sensitive uses, including for classified work and to support ongoing military operations. Add.28.

In fall 2025, petitioner and the Department began negotiations around deployment of petitioner's software on the Department's GenAI.mil platform. Add.30. In those discussions, the Department requested that petitioner permit the Department, "and its contractors and subcontractors, to use all versions of Claude for 'all lawful uses.'" Add.30-31; *cf.* Add.223

(reflecting the Secretary's determination that the Department must use AI "models free from usage policy constraints that may limit lawful military applications" and directing the relevant Under Secretary "to incorporate standard 'any lawful use' language into any [Department] contract through which AI services are procured").

Petitioner refused to agree to these terms. *See* Add.31. And over the course of negotiations, petitioner's behavior increasingly concerned the Department. In the Department's view, petitioner's insistence on maintaining an operational veto over the use of its software—along with its apparent unease about the potential that the software had been used in a particular military operation—raised concerns that petitioner might manipulate its software to enforce its own policy judgments about the Department's appropriate use. *See* Add.198-201.

Unable to resolve those issues, the Secretary on February 27 directed the Department to begin the process of designating petitioner a supply-chain risk pursuant to § 4713. Add.94. The Department evaluated the risks presented by petitioner and, on March 3, the Under Secretary of War for Acquisition and Sustainment and the Department's Chief Information

Officer jointly recommended that the Secretary invoke § 4713(c) to immediately designate petitioner a supply-chain risk. *See* Add.195-96.

The same day, the Secretary issued written determinations that: (1) the use of petitioner's products or services in the Department's systems "presents a significant supply chain risk" and the use of the § 4713(a) authority "is necessary to protect national security by reducing that" risk; (2) "no less intrusive measures" are "reasonably available to reduce" that risk; and (3) "an urgent national security interest requires the immediate exercise of the authority in Section 4713(a) pursuant to Section 4713(c)." Add.194. In addition, the Secretary determined that the designation would apply to all of petitioner's products and services covered by the statute and that the Secretary would take "all covered procurement actions" identified in the statute. *Id.*

The effect of that designation is that petitioner may not provide its products or services to the Department and that Department contractors may not use petitioner's products while working on Department contracts. *See* 41 U.S.C. § 4713(k)(4). The designation does not prohibit petitioner from contracting with other federal agencies or prohibit Department contractors

from using petitioner's products except as related to their work on Department contracts. *See id.*

Shortly after issuing his determination, the Secretary provided notice to petitioner. *See* Add.89-90. That notice explained that petitioner may request reconsideration and submit information or argument regarding such a request. *See* Add.90-91; *see also* 41 U.S.C. § 4713(b)(2), (c)(2)(A)-(B). Since that time, the Department has also—following internal review procedures required for releasing sensitive information—provided petitioner with the Secretary's determination and supporting materials. *See* Add.241-49.

After petitioner received notice—but before it received the determination or the supporting materials—petitioner filed a petition for review in this Court. *See* 41 U.S.C. § 1327(b). Petitioner raises various statutory and constitutional claims. *See* Pet. 2.[1] Petitioner has now moved for a stay pending review.

[1] Petitioner mentions other directives and actions by the President, the Secretary, and other federal agencies. Petitioner is challenging those actions in a separate suit; the only action subject to direct review in this Court is the Secretary's § 4713 designation.

ARGUMENT

A stay is an extraordinary remedy that "is not a matter of right." *Nken v. Holder*, 556 U.S. 418, 427 (2009) (quotations omitted). To obtain such relief, petitioner would need to justify a departure from "ordinary processes of administration and judicial review." *Id.* (quotations omitted). Petitioner fails to carry that burden. Petitioner has not shown likelihood of success on the merits, much less imminent irreparable harm that overcomes the countervailing national-security interests at stake. *See Winter v. Natural Res. Def. Council, Inc.*, 555 U.S. 7, 20, 32-33 (2008).

I. The Secretary's Supply Chain Risk Designation Addresses Significant National-Security Concerns

The Secretary has determined that the use of petitioner's products or services in any Department system—including systems used by contractors working on Department contracts—"presents a significant supply chain risk" that affects "urgent national security interest[s]" such that immediate designation was required. Add.194. The risk identified by the Secretary is the potential that petitioner will manipulate its AI model to "inhibit the [Department's] use," which would cause significant harm to the Department's "operational capabilities." Add.195.

As an initial matter, AI systems present "unique" risks because of the "opaque nature of the technology itself." Add.199. "Unlike traditional software," an AI model "require[s] constant tuning," and "AI systems are acutely vulnerable to manipulation." *Id.* Thus, a party with "[p]rivileged access" to the system—such as the vendor—can "subvert the design, integrity, and operation of the model." *Id.* As a result, the "integrity" of the system "is fundamentally based on the trustworthiness of the vendor." *Id.* If a vendor were "to unilaterally alter" the design of the system "without [the Department's] consent," those alterations could "fundamentally change the system's function and create[] a significant operational risk." *Id.* And given the ways in which AI systems are integrated into the Department's most sensitive capabilities—including ongoing military operations—those risks could materialize in "catastrophic downstream consequences, such as a critical defense system failing to engage." *Id.*

In this case, petitioner's conduct over time led the Secretary to doubt that petitioner was a trustworthy partner whose AI model could be relied on, particularly in the Department's extremely sensitive national-security systems. First, the Secretary has concluded that petitioner's attempt to contractually limit the lawful uses for which the Department may employ its

software reflects an "untenable" position that would improperly "restrict [the Department's] warfighting operations beyond the limitations imposed by law" and effectively grant petitioner "an operational veto" over the Department's most sensitive operations. Add.198. And petitioner's efforts to impose its own judgments about appropriate use of its software through contractual limits indicated that petitioner might develop additional "redlines" and restrict the Department's ability to use the software for other purposes, possibly without the Department's knowledge or consent. *See* Add.199-200.

Those concerns were compounded when one of petitioner's executives "questioned the propriety of the potential use of their software" via a prime contractor "for a sensitive military operation abroad despite that use being permitted under the existing Terms of Service." Add.198. That reaction to the use of petitioner's software "led to alarm by" both the Department and the prime contractor, raising "doubts" about whether—beyond the contractual limitations that petitioner continued to insist on—petitioner might "disallow[] its software to function in critical military operations" based on its own policy judgment. Add.198-99; *cf.* Add.34-35 (declaration from one of petitioner's co-founders explaining that petitioner's attempts to

limit the Department's use of its software reflect petitioner's own "technical judgment" and "principles").

And those reservations were further reinforced by the Secretary's judgment that petitioner's negotiation posture was "meant principally to benefit its public perception," even at the expense of the Department. Add.198. Petitioner's co-founder admits that petitioner resisted the Department's all-lawful-uses contractual term in part because acquiescing could undermine petitioner's standing "with customers, partners, investors, and the public," as well as its ability "to attract and retain" employees. Add.34. As the Secretary determined, when a vendor "treats its negotiations with the [Department] primarily as tools for brand-building"—including in ways "openly hostile" to the Department—that indicates a risk the vendor will restrict the Department's ability to use the vendor's software and thus undermines the necessary trust that must exist in this context. Add.198-99.

Based on that combination of actions, the Secretary determined that the Department and petitioner are unable "to establish the deep trust required for security collaboration." Add.199. Instead, the Secretary assessed that petitioner "can and would impose its moral and policy judgments on the warfighting capabilities of the" Department by

manipulating or restricting its software. Add.199-200. Thus, the Secretary concluded that "there is a substantial risk" that petitioner "could attempt to disable its technology or preemptively and surreptitiously alter the behavior of the model in advance or in the middle of ongoing warfighting operations" to enforce its "redlines." Add.200. And the Secretary deemed petitioner a significant supply chain risk to national security under § 4713. Add.194.

II. Petitioner Is Not Entitled to Emergency Relief

A. Petitioner's Premature Request for Relief Misapprehends the Designation

In its effort to manufacture an emergency, petitioner's motion rests on an incomplete legal and factual picture. Petitioner does not identify any source of law authorizing preliminary relief in this context. Under the relevant judicial review provision, this Court may "hold unlawful" actions that it determines to be "contrary to" law or "arbitrary" and "capricious." 41 U.S.C. § 1327(b)(2). But the statute makes clear that this determination "shall be the exclusive judicial remedy for any claim." *Id.* § 1327(b)(4)(C). And no provision grants the power to issue interim relief pending that final determination. *Compare* 5 U.S.C. § 705. This legislative choice fits within the broader scheme providing for review of vital national-security actions

with the benefit of the administrative record, which may include classified and other sensitive information. *See* 41 U.S.C. § 1327(b)(4)(B).

Indeed, petitioner lacked a full understanding of the circumstances when filing its motion. While petitioner surmised that the relevant agency officials prepared no joint recommendation assessing the risk, *see* Mot.12-13, the Secretary received and relied upon such a recommendation, *see* Add.194-96. Once the recommendation and supporting documents were approved for release, they were provided to petitioner. Although petitioner may have preferred to obtain the materials earlier, *see* Mot.13, 19 & n.3, the statute expressly contemplates temporarily delaying notice to the source where, as here, the agency "determines that an urgent national security interest [so] requires," 41 U.S.C. § 4713(c). And the Department will "promptly consider[] any information" that petitioner submits and decide whether "modifications to the determination" are appropriate "based on such information." *Id.* § 4713(c)(2)(B). These ongoing administrative processes provide further reason to defer judicial intervention at this juncture.

Petitioner's own motion illustrates many of the dangers of adjudication on a limited record. In asserting an absence of reasoning by the Department and speculating about the justifications for the designation, *see* Mot.14-17 &

n.2, petitioner did not have access to the Secretary's decision or supporting evidence. In the same vein, petitioner misunderstands the nature and scope of the designation. Relying on the Secretary's social media post that led to the designation process, petitioner claims that the Department has "require[d] other contractors to stop doing business with [petitioner]," Mot.17, and "threaten[ed] *any* commercial counterparty of [petitioner] that does business with the Department," Mot.23. But by its terms, the Secretary's designation—which is the sole action subject to review here—applies only to "[t]he use of any of [petitioner's] covered products or services in any [Department] covered system." Add.194. As petitioner's declarations appear to recognize, the Secretary may permissibly make such a decision to disallow an entity like petitioner from working on Department contracts. *See, e.g.*, Add.34 ("[B]ecause of Claude's limitations and safeguards, [the Department] may opt to work with another company that better suits its needs."); Add.54 ("[The Department] is of course able to use any other AI system that better meets its requirements.").

B. Petitioner Is Unlikely to Succeed on Its Challenges to the Designation

Petitioner asserts a grab-bag of objections to the Secretary's designation. Many are based on a misunderstanding of the basis for the

designation and the statutorily authorized emergency procedures the Secretary has followed. And the remainder are unlikely to succeed on the merits.

1. Petitioner's contentions (Mot.12-13, 15-17) that the Secretary failed to follow required procedures reflect petitioner's premature filing and incomplete knowledge of the facts. The Secretary properly invoked the authority in 41 U.S.C. § 4713(c) and followed all required procedures in issuing the designation.

The Secretary's designation reflects his determination "that an urgent national security interest requires the immediate exercise of the" designation authority under 41 U.S.C. § 4713(c). Add.194. And the Secretary followed the statute's procedures: He issued the determination only after receiving a joint recommendation from the relevant officials. Add.195-96; *see also* 41 U.S.C. § 4713(b)(1). He made written determinations that the use of petitioner's "covered products or services" in the Department's covered systems "presents a significant supply chain risk," that the § 4713 designation "is necessary to protect national security by reducing that" risk, and that "no less intrusive measures" are "reasonably available." Add.194; *see also* 41 U.S.C. § 4713(b)(3), (c)(1)(B). And he promptly provided notice of

the determination to the relevant Members of Congress and to petitioner. *See* Add.204-18; Add.241-49; *see also* 41 U.S.C. § 4713(c)(1)-(2) (allowing the Secretary to "temporarily delay" the required notice when an emergency determination is made).

Petitioner also erroneously contends that the Secretary's designation is unreasoned. These arguments largely stem from petitioner's decision to file its motion before receiving copies of the designation and supporting materials, which set forth the reasoned explanations that petitioner demands. *See* Add.195; Add.198-201. And to the extent that petitioner asks this Court to scrutinize the Secretary's national-security judgments on the merits, that request is inconsistent with the Supreme Court's repeated admonition that such judgments from the political branches are "entitled to deference" and ought not be lightly second-guessed by the judiciary. *Holder v. Humanitarian Law Project*, 561 U.S. 1, 33-35 (2010); *see also, e.g.*, *Trump v. Hawaii*, 585 U.S. 667, 704 (2018).

Each of petitioner's other arguments is unpersuasive. First, petitioner is wrong to contend (Mot.14, 16-17) that the Secretary's invocation of § 4713(c)'s emergency authority and the designation are inconsistent with the Department's previous use of Claude and with the Secretary's decision to

provide for a six-month transition period away from petitioner's products. The record reflects that petitioner's recent actions led the Department to assess the escalating national-security risks inherent in petitioner's insistence on effectively "grant[ing] itself an operational veto" on the use of its technology in military operations. Add.198; *see also* Add.200 ("Anthropic's risk level escalated from a potentially manageable technical and business negotiation to an unacceptable national security threat over the course of the [Department's] contract negotiation with them."). Exercising his national-security expertise, the Secretary determined that removing petitioner's products from the Department's systems immediately—in the middle of active military operations and before replacement products could be properly integrated into those systems—posed a greater risk to national security than did providing for an orderly transition period. *See* Add.233-34. And in the meantime, the Department "is taking additional measures to mitigate the supply chain risk," such as by "working with third-party cloud service providers to ensure Anthropic leadership cannot make unilateral changes to the" version of the software used by the Department. Add.235-36.

Nor does petitioner make headway when it briefly contends (Mot.16) that the risk identified by the Secretary is "worlds removed" from the kind of

risk contemplated by § 4713. The supply chain risk addressed by that statute encompasses broad risks arising from the possibility that "any person" may "manipulate the design, integrity, manufacturing, production, distribution, installation, operation, maintenance, disposition, or retirement" of an information-technology product to "deny, disrupt, or otherwise manipulate the function, use, or operation of" the product "or information stored on" the product. 41 U.S.C. § 4713(k)(6). Here, the Secretary identified the risk that petitioner may unilaterally manipulate its product to deny or disrupt the Department's ability to use the product for all lawful uses. That risk falls within the plain terms of the statute.

There is no textual basis for petitioner's argument that § 4713 may only be invoked to mitigate risks posed by "hostile nation states" or "foreign compan[ies]." Mot.16 (alteration and quotations omitted). The statute contemplates that the relevant risk may arise from the actions of "any person," 41 U.S.C. § 4713(k)(6)—in contrast to other statutes where Congress has authorized measures to address risks arising from activities of a "foreign person," *see, e.g.*, 50 U.S.C. § 4565(a)(4)(B), (d)(1), or a "foreign adversary," *see, e.g.*, Protecting Americans from Foreign Adversary Controlled Applications Act, Pub. L. No. 118-50, div. H, 138 Stat. 895 (2024).

Finally, petitioner's cursory challenge (Mot.17) to the Secretary's determination that less intrusive measures are not reasonably available lacks merit. As the record reflects, the risks involved stem from the possibility that petitioner could manipulate its software to constrain the Department's ability to carry out lawful military functions. *See* Add.198-201. That possibility includes circumstances where petitioner's software is used by a Department contractor working on Department contracts, because "there is a substantial risk that any company-imposed restrictions or alterations to the model would be transferred" to applications that the model is "layered into." Add.231-32. The Secretary reasonably determined that such a risk could only be ameliorated by prohibiting petitioner's software from use in any system working on Department contracts—not merely by removing petitioner's software from the Department's "classified systems" or by directly contracting with "other" companies in addition to, or instead of, petitioner. Mot.17.

2. Petitioner also incorrectly asserts that the Secretary's designation violated petitioner's due process rights. Here again, petitioner's premature motion misunderstands the relevant facts. In petitioner's view, it must be informed of "the factual basis for" the designation and be given "a

meaningful opportunity to rebut" those facts. Mot.18 (quotations omitted). But since petitioner filed its motion, the Department has provided petitioner with the designation and the supporting record, and petitioner now may provide any contrary evidence that it wishes the Secretary to consider. That sequencing is consistent with the procedures outlined in the statute, which permits the Secretary to "temporarily delay" providing notice when he finds (as he did here) "an urgent national security interest," 41 U.S.C. § 4713(c). And it ensures that petitioner will receive any process that is due.

Moreover, petitioner is wrong to the extent it implies (Mot.19 n.3) that such post-designation process is constitutionally insufficient. That suggestion would amount to an argument that the statute's delayed-notification procedures—which apply only when urgent national-security interests require prompt action—are unconstitutional. The single sentence in a footnote that petitioner devotes to this issue fails to meaningfully develop any basis on which this Court could invalidate an Act of Congress.

Regardless, on the merits, this Court and the Supreme Court have repeatedly recognized that, where the government "must act quickly," "postdeprivation process satisfies the requirements of the Due Process Clause." *Zevallos v. Obama*, 793 F.3d 106, 116 (D.C. Cir. 2015) (quoting

Gilbert v. Homar, 520 U.S. 924, 930 (1997)); *see also, e.g.*, *Zinermon v. Burch*, 494 U.S. 113, 128 (1990). Here, the statute allows the Secretary to delay providing notice when he determines that "an urgent national security interest requires" an immediately effective designation. 41 U.S.C. § 4713(c). That narrow statutory authority applies in precisely the sort of circumstances where this Court and the Supreme Court have recognized that delayed process is constitutionally sufficient, and petitioner's own authority (Mot.19 n.3) recognizes that "advance notification" of adverse action is not required where such "notification would impinge upon the security and other foreign policy goals of the United States." *People's Mojahedin Org. of Iran v. U.S. Dep't of State*, 613 F.3d 220, 227 n.4 (D.C. Cir. 2010) (per curiam) (quotations omitted).

The permissibility of this statutory post-designation process is particularly clear in this government-contracting context. In general, the government—like "private individuals and businesses"—"enjoys the unrestricted power" to "determine those with whom it will deal" and to "fix the terms and conditions upon which it will make needed purchases." *Perkins v. Lukens Steel Co.*, 310 U.S. 113, 127 (1940). And although this Court's precedents conclude that due process principles may be implicated

when the government "formally debar[s]" a party from government contracting writ large or otherwise "broadly precludes" a party "from a chosen trade or business," *Trifax Corp. v. District of Columbia*, 314 F.3d 641, 643-44 (D.C. Cir. 2003), the legal effect of the designation is more limited—it precludes petitioner's software from being used in the performance of Department contracts. The designation does not address the use of petitioner's software in contracts with other agencies, much less by private parties.

3. Petitioner is also unlikely to succeed on its First Amendment claims, which again stem from a misunderstanding of the relevant facts. In petitioner's telling, the Secretary's designation is the result of petitioner's engaging in various "protected activity," such as its "public statements regarding the importance of its safety limitations" and its "contribut[ions] to public discourse about safe use of AI models." Mot.19-20.

But that characterization is not supported by the facts. As the record shows, the Secretary was concerned about the possibility that petitioner would "disallow[] its software to function in critical military operations" and would "control the use of its product" in ways that restrict the Department's "lawful use" of it, including before or during "ongoing warfighting

operations." Add.198-200. That risk relates to petitioner's potential conduct, not its speech. And to the extent that the Secretary pointed to petitioner's speech as evidence that petitioner might engage in the injurious conduct, such evidentiary use of speech "is fully compatible with the First Amendment." *Flytenow, Inc. v. FAA*, 808 F.3d 882, 894 (D.C. Cir. 2015). Petitioner has failed to demonstrate that its protected speech, as divorced from its conduct, was a factor at all in the designation—much less that there is a sufficient "causal link" between that speech and the designation, *Aref v. Lynch*, 833 F.3d 242, 258 (D.C. Cir. 2016) (quotations omitted).

Petitioner's First Amendment argument is particularly unlikely to succeed in this context, where the government has not directly regulated petitioner's speech at all. Petitioner remains free to continue "contribut[ing] to public discourse about safe use of AI models," including by "posting public essays and blog posts" and by "supporting or opposing legislation." Mot.20. The Secretary has simply determined that the Department will not use its funds to purchase (directly or through other contractors) petitioner's software. In large part, petitioner identifies as the relevant "speech" petitioner's "refusal to acquiesce" to the contract terms that the Department insisted upon. Mot.21. But petitioner cites nothing in precedent or logic to

support the remarkable view that the government could violate the First Amendment by taking account of the contract terms that a potential counter-party will agree to in determining whether to contract with that party.

III. The Balance of Equities and Public Interest Preclude a Stay

Extraordinary relief is not warranted because petitioner identifies no exigency showing "a clear and present need for equitable relief to prevent irreparable harm." *Chaplaincy of Full Gospel Churches v. England*, 454 F.3d 290, 297 (D.C. Cir. 2006) (quotations omitted). And petitioner's asserted harms are far outweighed by the paramount interests in national security. *See Winter*, 555 U.S. at 23-24, 32-33 (holding that the public interest precluded a preliminary injunction regardless of the other factors).

Petitioner seeks to be excused from demonstrating concrete irreparable harm in light of its constitutional allegations. *See* Mot.22. Meritless constitutional claims do not support the entry of a stay. And petitioner's arguments fail on their own terms in any event. The status quo does not result in any "loss of First Amendment freedoms, for even minimal periods of time," *Elrod v. Burns*, 427 U.S. 347, 373 (1976), because the designation in no way hinders petitioner's ability to espouse whatever views it wishes. Petitioner's conclusory contentions are no substitute for

demonstrating "ongoing adverse effects to [its] First Amendment rights." *Media Matters for Am. v. Paxton*, 138 F.4th 563, 585 (D.C. Cir. 2025). Nor is this a case like *Karem v. Trump*, 960 F.3d 656 (D.C. Cir. 2020), where this Court concluded that adequate process was never afforded. Petitioner has received notice and an opportunity to submit materials for consideration by the agency.

Petitioner's asserted commercial harms depend on actions by independent actors not before the Court. *See* Mot.22-23. Petitioner's motion and declarations do not tie their injuries to the designation but instead refer to "the President's and Secretary's other actions" that are not—and cannot be—challenged in this proceeding. Mot.23; *see also* Add.65-68 (alleging effects from various government actions). Regardless, petitioner raises concerns that customers may choose not to use Claude based on general "fear" or "confusion" about "the repercussions" of doing so. Add.74. But conjecture about how third parties may react does not establish a remediable injury. *See Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 417 n.7 (2013). Indeed, it is difficult to see how the claimed harms would be rectified by a stay.

The stay request is all the more extraordinary because petitioner attempts to countermand the considered national-security judgments of top government officials. While petitioner's declarants disclaim any desire "to dictate how the government conducts its missions and who it works with," Add.34; *see* Add.54 (similar), petitioner simultaneously seeks to usurp the Department's determination that continued use of petitioner's AI model in military systems "pose[s] a serious threat to national security," *Winter*, 555 U.S. at 33. These complex decisions about operational needs and system requirements are entrusted to senior intelligence and military leaders.

Here, the Secretary acted under a statute designed to reduce risks from technology incorporated into government systems. *See* 41 U.S.C. § 4713. The government "suffers a form of irreparable injury" when it is prevented "from effectuating statutes enacted by representatives of its people." *Trump v. CASA, Inc.*, 606 U.S. 831, 861 (2025) (quotations omitted). That harm is especially pronounced here because the interest in ensuring the nation's security "is an urgent objective of the highest order." *Holder*, 561 U.S. at 28. Contrary to petitioner's contentions, the Department is not required to tolerate the risk that critical military systems will be jeopardized at pivotal moments for national defense and active military operations.

CONCLUSION

For the foregoing reasons, the Court should deny the motion for stay pending review.

Respectfully submitted,

BRETT A. SHUMATE
Assistant Attorney General
SHARON SWINGLE

/s/ Sean R. Janda
SEAN R. JANDA
BRIAN J. SPRINGER
Attorneys, Appellate Staff
Civil Division, Room 7260
U.S. Department of Justice
950 Pennsylvania Avenue NW
Washington, D.C. 20530
(202) 514-3388
sean.r.janda@usdoj.gov

MARCH 2026

CERTIFICATE OF COMPLIANCE

I hereby certify that the foregoing response complies with the word limit of Federal Rule of Appellate Procedure 27(d)(2)(A) because the response contains 5162 words. The response complies with the typeface and type-style requirements of Federal Rules of Appellate Procedure 27(d)(1)(E) and 32(a)(5) and (6) because it has been prepared using Microsoft Word 2016 in proportionally spaced 14-point CenturyExpd BT typeface.

/s/ Sean R. Janda
SEAN R. JANDA

CERTIFICATE OF SERVICE

I hereby certify that on March 19, 2026, I electronically filed the foregoing response with the Clerk of the Court for the United States Court of Appeals for the D.C. Circuit by using the appellate CM/ECF system. Participants in the case are registered CM/ECF users, and service will be accomplished by the appellate CM/ECF system.

/s/ Sean R. Janda
SEAN R. JANDA

ADDENDUM

TABLE OF CONTENTS

Page

~~CUI~~

SECRETARY OF WAR
1000 DEFENSE PENTAGON
WASHINGTON, DC 20301-1000

MAR - 3 2026

DETERMINATION

In accordance with Section 4713(c) of title 41, United States Code (U.S.C.), ("Section 4713"), and pursuant to the recommendation provided by the Under Secretary of War for Acquisition and Sustainment (USW(A&S)) and the Department of War Chief Information Officer (DoW CIO), I hereby determine that (i) the use of the authority set forth in Section 4713(a) with respect to a covered procurement involving Anthropic, PBC, and its subordinate, subsidiaries, or affiliated offices or entities, doing business under various names, and all subsidiaries, successors, or assigns thereof (the "Covered Entity"), is necessary to protect national security by reducing significant supply chain risk, (ii) less intrusive measures are not reasonably available to reduce such supply chain risk; and (iii) the use of such authorities will apply to a class of covered procurements.

Determination. In accordance with Section 4713(b)(3), based on the scoping analysis, mitigation considerations, and the joint recommendation of the DoW CIO and the USW(A&S) (Attached), I make the following determinations:

- **Covered Procurement Actions Are Necessary to Protect National Security**: The use of any of the Covered Entity's covered products or services in any DoW covered system presents a significant supply chain risk, and the use of the authority in Section 4713(a) is necessary to protect national security by reducing that supply chain risk.
- **No Less Intrusive Measures Are Reasonably Available:** There are no less intrusive measures that are reasonably available to reduce the supply chain risk associated with the use of the Covered Entity's products or services in any DoW covered system.
- **Class Determination:** The use of Section 4713 authorities will apply to all covered procurement actions involving the Covered Entity.

Scope and Applicability. This Determination is applicable to all of the Covered Entity's products or services that meet the definition of a "covered article" or that are part of a "covered procurement," as those terms are defined at 41 U.S.C. § 4713(k), whether acquired as a product or service. This includes all of the Covered Entity's products or services offered by the Covered Entity that become available for procurement.

Urgent National Security Interest. I have determined that an urgent national security interest requires the immediate exercise of the authority in Section 4713(a) pursuant to Section 4713(c). As such, DoW will take all action as required by Section 4713(b)-(c) following announcement of this determination.

Attachment:
As stated

Controlled By: OUSW(A&S) OASW(IBP)
CUI Category: OPSEC, PROPIN
LDC: D
POC: Vy Nguyen, Vy.K.Nguyen.civ@mail.mil

~~CUI~~

OFFICE OF THE SECRETARY OF WAR
1000 DEFENSE PENTAGON
WASHINGTON, DC 20301-1000

Joint Recommendation, Concurrence, and Determination to Use Section 4713 of Title 41, United States Code, Authorities to Mitigate Supply Chain Risk Related to Anthropic, PBC

Summary

This document sets forth the joint recommendation of the Under Secretary of War for Acquisition and Sustainment (USW(A&S)) and the Department of War Chief Information Officer (DoW CIO) for action to be undertaken pursuant to Section 4713 of title 41, United States Code (U.S.C.) ("Section 4713").

In accordance with Section 4713(b)(1), the USW(A&S) and DoW CIO consulted with procurement and other relevant officials within DoW and jointly recommend that there is a significant supply chain risk in a covered procurement[1] involving Anthropic, PBC, and its subordinate, subsidiaries, or affiliated offices or entities, doing business under various names, and all subsidiaries, successors, or assigns thereof (the "Covered Entity").

The Covered Entity's restrictions on the use of its products and services introduces significant national security risks to the DoW's supply chain.

Joint Recommendation by USW(A&S) and DoW CIO

Risk Analysis: The DoW CIO and USW(A&S) have determined the Covered Entity's restrictions on the use of its products and services pose unacceptable risk to the DoW. Specifically, there is significant risk, based upon the statements and actions of the Covered Entity, that use of its products and services and, as a result, the products and services of other entities with which DoW contracts, will be subject to manipulation in such a manner as to inhibit the DoW's use thereof. This creates significant risk to DoW's supply chain as the relevant products and services are integral to DoW's operational capabilities, as well as the functioning of various activities across the DoW. The DoW CIO and USW(A&S) therefore believe there is an urgent national security interest in mitigating the significant supply chain risk created by the Covered Entity as soon as practicable.

Joint USW(A&S)/DoW CIO Class Recommendation to Mitigate Supply Chain Risk: On the basis of this risk analysis and consultation with relevant DoW officials, the USW(A&S) and the DoW CIO jointly recommend that there is a significant supply chain risk associated with the use of the Covered Entity's products and services in any DoW covered system. DoW CIO and USW(A&S) therefore recommend invocation of the authorities codified at Section 4713(c) to urgently mitigate this risk as soon as practicable while minimizing disruption to the DoW.

[1] "Covered procurement" is defined at Section 4713(k)(3).

~~CUI~~

SIGNED:

HON Michael P. Duffey
Under Secretary of War for
Acquisition and Sustainment

Date: 3/3/26

HON Kirsten Davies
Department of War Chief
Information Officer

Date: 3 MARCH 2026

Attachment:
ATTACHMENT 1a – Urgent Supply Chain Risk Analysis on Anthropic PBC (~~CUI~~)
ATTACHMENT 1b – Due Diligence Preliminary Report on Anthropic (CUI//PROPIN)
ATTACHMENT 2 – Section 4713 Scoping Analysis for Anthropic, PBC

ATTACHMENT

1a

~~CUI~~

RESEARCH
AND ENGINEERING

UNDER SECRETARY OF WAR
3030 DEFENSE PENTAGON
WASHINGTON, DC 20301-3030

MEMORANDUM FOR THE RECORD

SUBJECT: Urgent Supply Chain Risk Analysis: Anthropic's Refusal to Permit Lawful AI Use

1. Summary

This analysis outlines the significant and unacceptable supply chain risk posed by Anthropic's unwillingness to agree to the U.S. government's use of its artificial intelligence (AI) models for lawful warfighting purposes. This unreasonableness endangers the strategic implementation and technical integrity of the Department of War's (DoW) information and related systems. Thus, this is not a mere contractual dispute. Anthropic's actions represent a direct challenge to the government's ability to control its own lawful operations and a threat to the security of the DoW's critical technology infrastructure. Anthropic's behavior therefore squarely meets the definition of "supply chain risk" as defined in both 10 U.S.C. § 3252 and 41 U.S.C. § 4713 and requires immediate mitigatory action.

2. The Operational and Strategic Threat

The government must ensure its technology assets are reliable, secure, and effective. Were DoW to accede to Anthropic's demands, the sought-after contract language would introduce a vendor-imposed point of failure. This is untenable. By embedding unreasonably restrictive terms that restrict DoW's warfighting operations beyond the limitations imposed by law, Anthropic seeks to grant itself an operational veto. This triggers the legal definition of supply chain risk at 10 U.S.C. § 3252(d)(4), which explicitly includes the risk that an entity may "deny, disrupt, or otherwise degrade the function, use, or operation" of a covered system. A contractual provision that unnecessarily restricts the use of a system to diminish functionality and limit DoW's warfighting capabilities introduces, by definition, an unreliable and compromised component into our warfighting mission.

This is compounded by demonstrated hostility in negotiations with DoW. Based on statements made during negotiations, Anthropic appears to be taking a negotiation posture meant principally to benefit its public perception that is not centered on truth or fact. In addition, during our negotiations, one of Anthropic's executives questioned the propriety of the potential use of their software for a sensitive military operation abroad despite that use being permitted under the existing Terms of Service. This led to alarm by the DoW and the prime contractor who provides Anthropic software, and raised material doubts as to whether they would cause their software to stop working or cause some other disastrous action that would put our warfighters lives in danger. The DoW recognizes that its suppliers are often for-profit corporations that intend both to help the warfighters and American public and turn a profit. However, a vendor that raises the prospect of disallowing its software to function in critical military operations, and treats its

~~CUI~~

~~CUI~~

RESEARCH
AND ENGINEERING

UNDER SECRETARY OF WAR
3030 DEFENSE PENTAGON
WASHINGTON, DC 20301-3030

negotiations with the DoW primarily as tools for brand-building cannot be trusted, particularly when that marketing campaign is openly hostile to the DoW and duplicitous. By ceding to Anthropic's terms, the DoW would be allowing the very corporate decisionmakers who have opted to publicly spat with DoW into its technical and operational warfighting infrastructure, thereby introducing unnecessary risk into DoW supply chains. The American people have vested elected officials and military and civilian leadership with warfighting authorities; it is untenable and unlawful to insert unelected corporate bureaucrats into this process.

3. The Underlying Technical Vulnerability of AI

This strategic risk is magnified by the unique, opaque nature of the technology itself. Unlike traditional software, AI models are probabilistic systems which are understood to "drift" or degrade as new data is introduced and require constant tuning, the integrity of which, is fundamentally based on the trustworthiness of the vendor to ensure the model continues to perform accurately and fairly.

The DoW cannot trust Anthropic to ensure the integrity of its models. As research demonstrates,[1] AI systems are acutely vulnerable to manipulation. Privileged access with malintent can subtly poison the training data to maliciously introduce unwanted function, or otherwise subvert the design, integrity, and operation of the model. Research shows such attacks can degrade accuracy by over 27% and introduce targeted misclassifications at an alarming rate.[2] Anthropic's ability to unilaterally alter system guardrails and model weights without DoW consent could fundamentally change the system's function and creates a significant operational risk. This could create catastrophic downstream consequences, such as a critical defense system failing to engage due to an unapproved, vendor-side modification. In August 2025, Anthropic itself disclosed that hackers had used its chatbot, Claude, to write code capable of carrying out cyberattacks against at least 17 organizations, including government entities noting that Agentic AI has been weaponized.[3]

A vendor like Anthropic, which has already demonstrated a hostile and non-cooperative stance on the use of its product, has the motive, means, and opportunity to introduce such vulnerabilities. Its refusal to partner in good faith makes it impossible to establish the deep trust required for security collaboration. The DoW would be forced to operate a black box controlled by a hostile party, which could contain hidden biases or backdoors. A vendor that seeks to control the use of its product so as to restrict DoW's lawful use thereof cannot be trusted. Given the public statements of Anthropic's CEO and others associated with the company, the

[1] See e.g. 2025 PhotonIcs & Electromagnetics Research Symposium, Abu Dhabi, UAE, 4-8 May PIERS Detecting and Preventing Data Poisoning Attacks on AI Models
[2] Id.
[3] anthropic.com/news/detecting-countering-misuse-aug-2025#:~:text=No-code%20malware:%20selling%20AI,with%20third-party%20safety%20teams.

~~CUI~~

~~CUI~~

RESEARCH
AND ENGINEERING

UNDER SECRETARY OF WAR
3030 DEFENSE PENTAGON
WASHINGTON, DC 20301-3030

Department must assume that Anthropic can and would impose its moral and policy judgments on the warfighting capabilities of the DoW, and therefore there is a substantial risk that Anthropic could attempt to disable its technology or preemptively and surreptitiously alter the behavior of the model in advance or in the middle of ongoing warfighting operations, if it feels that its "redlines" are crossed. The threat of such an action is unacceptable.

4. Progression of Risk

The DoW institutes the U.S. Government standard Risk Management Framework (RMF) across all layers of technology, assets, data, processes, and supply chain. In accordance with the DoW RMF, assessments result in areas of risk across the DoW ecosystem (including vendors). Though an individual vendor may have only limited risk in individual categories, the aggregation of risk across categories can result in a vendor being deemed high risk. In other words, the culmination of unmitigable risks lead to a vendor having a material level of risk. The vendor can then be deemed a "supply chain risk," at which time they typically are removed from applicable systems to mitigate issues and threats.

In the instant case, Anthropic's risk level escalated from a potentially manageable technical and business negotiation to an unacceptable national security threat over the course of the DoW's contract negotiation with them. Given the nature of AI systems and Anthropic's privileged access as the AI model's developer, curator and maintainer, there was a baseline risk given the potential harmful actions this privileged technical access makes possible. The supply chain risk level increased when Anthropic insisted on terms of service that would constrain the DoW beyond what is in the law. This risk further increased when Anthropic asserted in the negotiations that it have an approval role in the operational decision chain, which would require the DoW to accept significant operational risk. Then during the final weeks of negotiations, it became clear that Anthropic was leveraging the DoW's ongoing good faith negotiations for Anthropic's own public relations, and they began engaging in an increasingly hostile manner through the press, despite the ongoing private negotiations with DoW leadership. Finally, this hostile posture was even further compounded when, during a time of active military operations, Anthropic leadership questioned the use of their technology in our warfighting systems clearly permitted under the Terms of Service of their existing contract with our Prime contractor. This collective set of actions represents a fully mature supply chain risk – including increased potential for model poisoning, insider threat risk, data exfiltration, and denial of service – posing a direct, intolerable, and material risk to our warfighting capability which warrants the designation of Anthropic as a supply chain risk.

~~CUI~~

~~CUI~~

RESEARCH
AND ENGINEERING

UNDER SECRETARY OF WAR
3030 DEFENSE PENTAGON
WASHINGTON, DC 20301-3030

5. Conclusion and Justification for Action

Anthropic's position is not a simple policy disagreement; it is an active demonstration of the exact risks our supply chain risk management laws were written to prevent. Use of Anthropic's products or services introduces significant risk to the DoW's covered systems, as the vendor, by maintaining the ability and necessity to continuously update and tune the product enables the potential for the vendor to subvert the design and/or functionality of their product or service. Such ability by the vendor could be used to implement changes in alignment with the vendor's ideology, putting the Department's lawful use of the capability at risk.

Therefore, Anthropic's unwillingness to permit the use of its technology to the extent permitted by law creates a clear and present supply chain risk as defined in 10 U.S.C. § 3252 and 41 U.S.C. § 4713.

Emil Michael

~~CUI~~

ATTACHMENT 2

ATTACHMENT
Section 4713 Scoping Analysis for Anthropic, PBC

This document supports the use of section 4713 of title 41, United States Code ("Section 4713') authorities. The Secretary of War, pursuant to the recommendation of the Under Secretary of War for Acquisition and Sustainment and the Department of War Chief Information Officer, has determined the following as the appropriate scope for use of Section 4713 authorities necessary to address the supply chain risk related to the use of covered products or services of Anthropic, PBC:

- **Covered Entity:** Anthropic, PBC, and its subordinate, subsidiaries, or affiliated offices or entities, doing business under various names, and all subsidiaries, successors, or assigns thereof ("Covered Entity").

- **Covered Products or Services:** All of the Covered Entity's products or services that meet the definition of a "covered article" or that are part of a "covered procurement," as those terms are defined at 41 U.S.C. § 4713(k), whether acquired as a product or service. This includes all of the Covered Entity's products or services offered by the Covered Entity that become available for procurement.

- **Covered Procurements:** All DoW procurements described in Section 4713(k)(3).

- **Covered Procurement Actions:** All actions described in Section 4713(k)(4).

SECRETARY OF WAR
1000 DEFENSE PENTAGON
WASHINGTON, DC 20301-1000

MAR - 3 2026

The Honorable Mike D. Rogers
Chairman
Committee on Armed Services
U.S. House of Representatives
Washington, DC 20515

Dear Mr. Chairman:

In accordance with title 41, U.S. Code, section 4713, I am notifying you of my determination that the use of products or services of Anthropic, PBC, including its subordinate, subsidiary, and affiliated offices or entities, doing business under various names, and all successors or assigns thereof (the "Covered Entity") in Department of War (DoW) covered procurements[1] presents a significant supply chain risk and that the use of section 4713 authorities is necessary to protect our national security. This determination is based in part on a risk analysis by the DoW and input from senior DoW personnel that the Covered Entity's restrictions on the use of its products and services introduces national security risks to the DoW's supply chain.

I have consulted with procurement and other relevant officials within DoW regarding the Covered Entity and determined that (i) use of the authority provided in section 4713 to carry out covered procurement actions[2] is necessary to protect national security by reducing supply chain risk, and (ii) less intrusive measures are not reasonably available to reduce such supply chain risk. Accordingly, this letter is providing notice of a section 4713 determination regarding the products and services of the Covered Entity.

I am sending identical letters to Congress and the appropriate congressional committees.

Sincerely,

PBH

cc:
The Honorable Adam Smith
Ranking Member

[1] Section 4713(k)(3).
[2] Section 4713(k)(4).

SECRETARY OF WAR
1000 DEFENSE PENTAGON
WASHINGTON, DC 20301-1000

MAR - 3 2026

The Honorable Roger F. Wicker
Chairman
Committee on Armed Services
United States Senate
Washington, DC 20510

Dear Mr. Chairman:

In accordance with title 41, U.S. Code, section 4713, I am notifying you of my determination that the use of products or services of Anthropic, PBC, including its subordinate, subsidiary, and affiliated offices or entities, doing business under various names, and all successors or assigns thereof (the "Covered Entity") in Department of War (DoW) covered procurements[1] presents a significant supply chain risk and that the use of section 4713 authorities is necessary to protect our national security. This determination is based in part on a risk analysis by the DoW and input from senior DoW personnel that the Covered Entity's restrictions on the use of its products and services introduces national security risks to the DoW's supply chain.

I have consulted with procurement and other relevant officials within DoW regarding the Covered Entity and determined that (i) use of the authority provided in section 4713 to carry out covered procurement actions[2] is necessary to protect national security by reducing supply chain risk, and (ii) less intrusive measures are not reasonably available to reduce such supply chain risk. Accordingly, this letter is providing notice of a section 4713 determination regarding the products and services of the Covered Entity.

I am sending identical letters to Congress and the appropriate congressional committees.

Sincerely,

PBH

cc:
The Honorable Jack Reed
Ranking Member

[1] Section 4713(k)(3).
[2] Section 4713(k)(4).

SECRETARY OF WAR
1000 DEFENSE PENTAGON
WASHINGTON, DC 20301-1000

MAR - 3 2026

The Honorable Susan M. Collins
Chair
Committee on Appropriations
United States Senate
Washington, DC 20510

Dear Madam Chair:

In accordance with title 41, U.S. Code, section 4713, I am notifying you of my determination that the use of products or services of Anthropic, PBC, including its subordinate, subsidiary, and affiliated offices or entities, doing business under various names, and all successors or assigns thereof (the "Covered Entity") in Department of War (DoW) covered procurements[1] presents a significant supply chain risk and that the use of section 4713 authorities is necessary to protect our national security. This determination is based in part on a risk analysis by the DoW and input from senior DoW personnel that the Covered Entity's restrictions on the use of its products and services introduces national security risks to the DoW's supply chain.

I have consulted with procurement and other relevant officials within DoW regarding the Covered Entity and determined that (i) use of the authority provided in section 4713 to carry out covered procurement actions[2] is necessary to protect national security by reducing supply chain risk, and (ii) less intrusive measures are not reasonably available to reduce such supply chain risk. Accordingly, this letter is providing notice of a section 4713 determination regarding the products and services of the Covered Entity.

I am sending identical letters to Congress and the appropriate congressional committees.

Sincerely,

PBH

cc:
The Honorable Patty L. Murray
Vice Chair

[1] Section 4713(k)(3).
[2] Section 4713(k)(4).

SECRETARY OF WAR
1000 DEFENSE PENTAGON
WASHINGTON, DC 20301-1000

MAR - 3 2026

The Honorable Tom J. Cole
Chairman
Committee on Appropriations
U.S. House of Representatives
Washington, DC 20515

Dear Mr. Chairman:

In accordance with title 41, U.S. Code, section 4713, I am notifying you of my determination that the use of products or services of Anthropic, PBC, including its subordinate, subsidiary, and affiliated offices or entities, doing business under various names, and all successors or assigns thereof (the "Covered Entity") in Department of War (DoW) covered procurements[1] presents a significant supply chain risk and that the use of section 4713 authorities is necessary to protect our national security. This determination is based in part on a risk analysis by the DoW and input from senior DoW personnel that the Covered Entity's restrictions on the use of its products and services introduces national security risks to the DoW's supply chain.

I have consulted with procurement and other relevant officials within DoW regarding the Covered Entity and determined that (i) use of the authority provided in section 4713 to carry out covered procurement actions[2] is necessary to protect national security by reducing supply chain risk, and (ii) less intrusive measures are not reasonably available to reduce such supply chain risk. Accordingly, this letter is providing notice of a section 4713 determination regarding the products and services of the Covered Entity.

I am sending identical letters to Congress and the appropriate congressional committees.

Sincerely,

PBH

cc:
The Honorable Rosa L. DeLauro
Ranking Member

[1] Section 4713(k)(3).
[2] Section 4713(k)(4).

SECRETARY OF WAR
1000 DEFENSE PENTAGON
WASHINGTON, DC 20301-1000

MAR - 3 2026

The Honorable Rick Crawford
Chairman
Permanent Select Committee on Intelligence
U.S. House of Representatives
Washington, DC 20515

Dear Mr. Chairman:

In accordance with title 41, U.S. Code, section 4713, I am notifying you of my determination that the use of products or services of Anthropic, PBC, including its subordinate, subsidiary, and affiliated offices or entities, doing business under various names, and all successors or assigns thereof (the "Covered Entity") in Department of War (DoW) covered procurements[1] presents a significant supply chain risk and that the use of section 4713 authorities is necessary to protect our national security. This determination is based in part on a risk analysis by the DoW and input from senior DoW personnel that the Covered Entity's restrictions on the use of its products and services introduces national security risks to the DoW's supply chain.

I have consulted with procurement and other relevant officials within DoW regarding the Covered Entity and determined that (i) use of the authority provided in section 4713 to carry out covered procurement actions[2] is necessary to protect national security by reducing supply chain risk, and (ii) less intrusive measures are not reasonably available to reduce such supply chain risk. Accordingly, this letter is providing notice of a section 4713 determination regarding the products and services of the Covered Entity.

I am sending identical letters to Congress and the appropriate congressional committees.

Sincerely,

PBH

cc:
The Honorable Jim Himes
Ranking Member

[1] Section 4713(k)(3).
[2] Section 4713(k)(4).

SECRETARY OF WAR
1000 DEFENSE PENTAGON
WASHINGTON, DC 20301-1000

MAR - 3 2026

The Honorable Tom Cotton
Chairman
Select Committee on Intelligence
United States Senate
Washington, DC 20510

Dear Mr. Chairman:

In accordance with title 41, U.S. Code, section 4713, I am notifying you of my determination that the use of products or services of Anthropic, PBC, including its subordinate, subsidiary, and affiliated offices or entities, doing business under various names, and all successors or assigns thereof (the "Covered Entity") in Department of War (DoW) covered procurements[1] presents a significant supply chain risk and that the use of section 4713 authorities is necessary to protect our national security. This determination is based in part on a risk analysis by the DoW and input from senior DoW personnel that the Covered Entity's restrictions on the use of its products and services introduces national security risks to the DoW's supply chain.

I have consulted with procurement and other relevant officials within DoW regarding the Covered Entity and determined that (i) use of the authority provided in section 4713 to carry out covered procurement actions[2] is necessary to protect national security by reducing supply chain risk, and (ii) less intrusive measures are not reasonably available to reduce such supply chain risk. Accordingly, this letter is providing notice of a section 4713 determination regarding the products and services of the Covered Entity.

I am sending identical letters to Congress and the appropriate congressional committees.

Sincerely,

PBH

cc:
The Honorable Mark Warner
Vice Chairman

[1] Section 4713(k)(3).
[2] Section 4713(k)(4).

SECRETARY OF WAR
1000 DEFENSE PENTAGON
WASHINGTON, DC 20301-1000

MAR - 3 2026

The Honorable Rand Paul
Chairman
Committee on Homeland Security and
Governmental Affairs
United States Senate
Washington, DC 20510

Dear Mr. Chairman:

In accordance with title 41, U.S. Code, section 4713, I am notifying you of my determination that the use of products or services of Anthropic, PBC, including its subordinate, subsidiary, and affiliated offices or entities, doing business under various names, and all successors or assigns thereof (the "Covered Entity") in Department of War (DoW) covered procurements[1] presents a significant supply chain risk and that the use of section 4713 authorities is necessary to protect our national security. This determination is based in part on a risk analysis by the DoW and input from senior DoW personnel that the Covered Entity's restrictions on the use of its products and services introduces national security risks to the DoW's supply chain.

I have consulted with procurement and other relevant officials within DoW regarding the Covered Entity and determined that (i) use of the authority provided in section 4713 to carry out covered procurement actions[2] is necessary to protect national security by reducing supply chain risk, and (ii) less intrusive measures are not reasonably available to reduce such supply chain risk. Accordingly, this letter is providing notice of a section 4713 determination regarding the products and services of the Covered Entity.

I am sending identical letters to Congress and the appropriate congressional committees.

Sincerely,

PBH

cc:
The Honorable Gary C. Peters
Ranking Member

[1] Section 4713(k)(3).
[2] Section 4713(k)(4).

SECRETARY OF WAR
1000 DEFENSE PENTAGON
WASHINGTON, DC 20301-1000

MAR - 3 2026

The Honorable James R. Comer
Chairman
Committee on Oversight and Government Reform
U.S. House of Representatives
Washington, DC 20515

Dear Mr. Chairman:

In accordance with title 41, U.S. Code, section 4713, I am notifying you of my determination that the use of products or services of Anthropic, PBC, including its subordinate, subsidiary, and affiliated offices or entities, doing business under various names, and all successors or assigns thereof (the "Covered Entity") in Department of War (DoW) covered procurements[1] presents a significant supply chain risk and that the use of section 4713 authorities is necessary to protect our national security. This determination is based in part on a risk analysis by the DoW and input from senior DoW personnel that the Covered Entity's restrictions on the use of its products and services introduces national security risks to the DoW's supply chain.

I have consulted with procurement and other relevant officials within DoW regarding the Covered Entity and determined that (i) use of the authority provided in section 4713 to carry out covered procurement actions[2] is necessary to protect national security by reducing supply chain risk, and (ii) less intrusive measures are not reasonably available to reduce such supply chain risk. Accordingly, this letter is providing notice of a section 4713 determination regarding the products and services of the Covered Entity.

I am sending identical letters to Congress and the appropriate congressional committees.

Sincerely,

PBH

cc:
The Honorable Robert Garcia
Ranking Member

[1] Section 4713(k)(3).
[2] Section 4713(k)(4).

SECRETARY OF WAR
1000 DEFENSE PENTAGON
WASHINGTON, DC 20301-1000

MAR - 3 2026

The Honorable Chuck Grassley
Chairman
Committee on the Judiciary
United States Senate
Washington, DC 20510

Dear Mr. Chairman:

In accordance with title 41, U.S. Code, section 4713, I am notifying you of my determination that the use of products or services of Anthropic, PBC, including its subordinate, subsidiary, and affiliated offices or entities, doing business under various names, and all successors or assigns thereof (the "Covered Entity") in Department of War (DoW) covered procurements[1] presents a significant supply chain risk and that the use of section 4713 authorities is necessary to protect our national security. This determination is based in part on a risk analysis by the DoW and input from senior DoW personnel that the Covered Entity's restrictions on the use of its products and services introduces national security risks to the DoW's supply chain.

I have consulted with procurement and other relevant officials within DoW regarding the Covered Entity and determined that (i) use of the authority provided in section 4713 to carry out covered procurement actions[2] is necessary to protect national security by reducing supply chain risk, and (ii) less intrusive measures are not reasonably available to reduce such supply chain risk. Accordingly, this letter is providing notice of a section 4713 determination regarding the products and services of the Covered Entity.

I am sending identical letters to Congress and the appropriate congressional committees.

Sincerely,

PBH

cc:
The Honorable Dick Durbin
Ranking Member

[1] Section 4713(k)(3).
[2] Section 4713(k)(4).

SECRETARY OF WAR
1000 DEFENSE PENTAGON
WASHINGTON, DC 20301-1000

MAR - 3 2026

The Honorable Jim Jordan
Chairman
Committee on the Judiciary
U.S. House of Representatives
Washington, DC 20515

Dear Mr. Chairman:

In accordance with title 41, U.S. Code, section 4713, I am notifying you of my determination that the use of products or services of Anthropic, PBC, including its subordinate, subsidiary, and affiliated offices or entities, doing business under various names, and all successors or assigns thereof (the "Covered Entity") in Department of War (DoW) covered procurements[1] presents a significant supply chain risk and that the use of section 4713 authorities is necessary to protect our national security. This determination is based in part on a risk analysis by the DoW and input from senior DoW personnel that the Covered Entity's restrictions on the use of its products and services introduces national security risks to the DoW's supply chain.

I have consulted with procurement and other relevant officials within DoW regarding the Covered Entity and determined that (i) use of the authority provided in section 4713 to carry out covered procurement actions[2] is necessary to protect national security by reducing supply chain risk, and (ii) less intrusive measures are not reasonably available to reduce such supply chain risk. Accordingly, this letter is providing notice of a section 4713 determination regarding the products and services of the Covered Entity.

I am sending identical letters to Congress and the appropriate congressional committees.

Sincerely,

PBH

cc:
The Honorable Jamie Raskin
Ranking Member

[1] Section 4713(k)(3).
[2] Section 4713(k)(4).

SECRETARY OF WAR
1000 DEFENSE PENTAGON
WASHINGTON, DC 20301-1000

MAR - 3 2026

The Honorable Andrew Garbarino
Chairman
Committee on Homeland Security
U.S. House of Representatives
Washington, DC 20515

Dear Mr. Chairman,

In accordance with title 41, U.S. Code, section 4713, I am notifying you of my determination that the use of products or services of Anthropic, PBC, including its subordinate, subsidiary, and affiliated offices or entities, doing business under various names, and all successors or assigns thereof (the "Covered Entity") in Department of War (DoW) covered procurements[1] presents a significant supply chain risk and that the use of section 4713 authorities is necessary to protect our national security. This determination is based in part on a risk analysis by the DoW and input from senior DoW personnel that the Covered Entity's restrictions on the use of its products and services introduces national security risks to the DoW's supply chain.

I have consulted with procurement and other relevant officials within DoW regarding the Covered Entity and determined that (i) use of the authority provided in section 4713 to carry out covered procurement actions[2] is necessary to protect national security by reducing supply chain risk, and (ii) less intrusive measures are not reasonably available to reduce such supply chain risk. Accordingly, this letter is providing notice of a section 4713 determination regarding the products and services of the Covered Entity.

I am sending identical letters to Congress and the appropriate congressional committees.

Sincerely,

PBH

cc:
The Honorable Bennie G. Thompson
Ranking Member

[1] Section 4713(k)(3).
[2] Section 4713(k)(4).

SECRETARY OF WAR
1000 DEFENSE PENTAGON
WASHINGTON, DC 20301-1000

MAR - 3 2026

The Honorable Ted Cruz
Chairman
Committee on Commerce, Science, and Transportation
United States Senate
Washington, DC 20510

Dear Mr. Chairman:

In accordance with title 41, U.S. Code, section 4713, I am notifying you of my determination that the use of products or services of Anthropic, PBC, including its subordinate, subsidiary, and affiliated offices or entities, doing business under various names, and all successors or assigns thereof (the "Covered Entity") in Department of War (DoW) covered procurements[1] presents a significant supply chain risk and that the use of section 4713 authorities is necessary to protect our national security. This determination is based in part on a risk analysis by the DoW and input from senior DoW personnel that the Covered Entity's restrictions on the use of its products and services introduces national security risks to the DoW's supply chain.

I have consulted with procurement and other relevant officials within DoW regarding the Covered Entity and determined that (i) use of the authority provided in section 4713 to carry out covered procurement actions[2] is necessary to protect national security by reducing supply chain risk, and (ii) less intrusive measures are not reasonably available to reduce such supply chain risk. Accordingly, this letter is providing notice of a section 4713 determination regarding the products and services of the Covered Entity.

I am sending identical letters to Congress and the appropriate congressional committees.

Sincerely,

PBH

cc:
The Honorable Maria Cantwell
Ranking Member

[1] Section 4713(k)(3).
[2] Section 4713(k)(4).

SECRETARY OF WAR
1000 DEFENSE PENTAGON
WASHINGTON, DC 20301-1000

MAR - 3 2026

The Honorable Brett Guthrie
Chairman
Committee on Energy and Commerce
U.S. House of Representatives
Washington, DC 20515

Dear Mr. Chairman:

In accordance with title 41, U.S. Code, section 4713, I am notifying you of my determination that the use of products or services of Anthropic, PBC, including its subordinate, subsidiary, and affiliated offices or entities, doing business under various names, and all successors or assigns thereof (the "Covered Entity") in Department of War (DoW) covered procurements[1] presents a significant supply chain risk and that the use of section 4713 authorities is necessary to protect our national security. This determination is based in part on a risk analysis by the DoW and input from senior DoW personnel that the Covered Entity's restrictions on the use of its products and services introduces national security risks to the DoW's supply chain.

I have consulted with procurement and other relevant officials within DoW regarding the Covered Entity and determined that (i) use of the authority provided in section 4713 to carry out covered procurement actions[2] is necessary to protect national security by reducing supply chain risk, and (ii) less intrusive measures are not reasonably available to reduce such supply chain risk. Accordingly, this letter is providing notice of a section 4713 determination regarding the products and services of the Covered Entity.

I am sending identical letters to Congress and the appropriate congressional committees.

Sincerely,

PBH

cc:
The Honorable Frank Pallone, Jr.
Ranking Member

[1] Section 4713(k)(3).
[2] Section 4713(k)(4).

SECRETARY OF WAR
1000 DEFENSE PENTAGON
WASHINGTON, DC 20301-1000

MAR - 3 2026

The Honorable John Thune
Senate Majority Leader
United States Senate
Washington, DC 20510

Dear Mr. Majority Leader:

In accordance with title 41, U.S. Code, section 4713, I am notifying you of my determination that the use of products or services of Anthropic, PBC, including its subordinate, subsidiary, and affiliated offices or entities, doing business under various names, and all successors or assigns thereof (the "Covered Entity") in Department of War (DoW) covered procurements[1] presents a significant supply chain risk and that the use of section 4713 authorities is necessary to protect our national security. This determination is based in part on a risk analysis by the DoW and input from senior DoW personnel that the Covered Entity's restrictions on the use of its products and services introduces national security risks to the DoW's supply chain.

I have consulted with procurement and other relevant officials within DoW regarding the Covered Entity and determined that (i) use of the authority provided in section 4713 to carry out covered procurement actions[2] is necessary to protect national security by reducing supply chain risk, and (ii) less intrusive measures are not reasonably available to reduce such supply chain risk. Accordingly, this letter is providing notice of a section 4713 determination regarding the products and services of the Covered Entity.

I am sending identical letters to Congress and the appropriate congressional committees.

Sincerely,

PBH

cc:
The Honorable Charles E. Schumer
Minority Leader

[1] Section 4713(k)(3).
[2] Section 4713(k)(4).

SECRETARY OF WAR
1000 DEFENSE PENTAGON
WASHINGTON, DC 20301-1000

MAR - 3 2026

The Honorable Mike Johnson
Speaker of the House
U.S. House of Representatives
Washington, DC 20515

Dear Mr. Speaker:

In accordance with title 41, U.S. Code, section 4713, I am notifying you of my determination that the use of products or services of Anthropic, PBC, including its subordinate, subsidiary, and affiliated offices or entities, doing business under various names, and all successors or assigns thereof (the "Covered Entity") in Department of War (DoW) covered procurements[1] presents a significant supply chain risk and that the use of section 4713 authorities is necessary to protect our national security. This determination is based in part on a risk analysis by the DoW and input from senior DoW personnel that the Covered Entity's restrictions on the use of its products and services introduces national security risks to the DoW's supply chain.

I have consulted with procurement and other relevant officials within DoW regarding the Covered Entity and determined that (i) use of the authority provided in section 4713 to carry out covered procurement actions[2] is necessary to protect national security by reducing supply chain risk, and (ii) less intrusive measures are not reasonably available to reduce such supply chain risk. Accordingly, this letter is providing notice of a section 4713 determination regarding the products and services of the Covered Entity.

I am sending identical letters to Congress and the appropriate congressional committees.

Sincerely,

PBH

cc:
The Honorable Hakeem Jeffries
Minority Leader

[1] Section 4713(k)(3).
[2] Section 4713(k)(4).

SECRETARY OF WAR
1000 DEFENSE PENTAGON
WASHINGTON, DC 20301-1000

JAN - 9 2026

MEMORANDUM FOR SENIOR PENTAGON LEADERSHIP
COMMANDERS OF THE COMBATANT COMMANDS
DEFENSE AGENCY AND DOW FIELD ACTIVITY DIRECTORS

SUBJECT: Artificial Intelligence Strategy for the Department of War

Accelerating America's Military AI Dominance

President Trump makes clear in Executive Order 14179, "It is the policy of the United States to sustain and enhance America's global Artificial Intelligence (AI) dominance in order to promote human flourishing, economic competitiveness, and national security." In the national security domain, AI-enabled warfare and AI-enabled capability development will re-define the character of military affairs over the next decade. This transformation is a race — fueled by the accelerating pace of commercial AI innovation coming out of America's private sector. The United States Military must build on its lead over our adversaries in integrating this technology, established during President Trump's first term, to make our Warfighters more lethal and efficient. To this end, aligned with America's AI Action Plan, I direct the Department of War to accelerate America's Military AI Dominance by becoming an "AI-first" warfighting force across all components, from front to back.

The Department will achieve this objective by:

- Unleashing experimentation with America's leading AI models Department-wide, and rewarding AI-first re-conceptions of legacy approaches;
- Aggressively identifying and eliminating bureaucratic barriers to deeper integration, which are vestiges of legacy information technology and modes of warfare;
- Focusing our investment to leverage America's core asymmetric advantages in AI computing, model innovation, entrepreneurial dynamism, capital markets, and combat-proven operational data from two decades of military and intelligence operations that no other military can replicate; and
- Executing a set of "Pace-Setting Projects" (PSPs) that will demonstrate the accelerated pace of execution, focus, and ethos we need to stay ahead. The PSPs will also serve as tangible, outcome-oriented vehicles for rapidly completing our buildout of the foundational AI enablers (infrastructure, data, models, policies, and talent) needed to accelerate AI integration across the entire Department.

The seven initial PSPs outlined below establish the new execution standard: single accountable leaders, aggressive timelines, measurable outcomes, and rapid iteration where failure accelerates learning and improvement.

Acceleration Approach

The means we will employ to pursue this strategy will continue to encompass our substantial program funding and workforce focused on AI across the Services and Components. We will also use the timely financial resources provided by Congress in the form of One Big Beautiful Bill, along with expanded budget withhold (Joint Acceleration Reserve) flexibility, to catalyze our accelerated pace of Military AI integration in the immediate term. And we will leverage the access, capabilities, investments, and insights of America's allies and partners to support our shared objectives, consistent with the President Trump's AI Action Plan to "Lead in International AI Diplomacy and Security".

We will re-focus the Chief Digital and AI Office (CDAO) and these enhanced resources to unlock critical foundational enablers needed to accelerate war-winning efforts across the Department, starting with enabling the set of seven PSPs listed below in fiscal year 2026. These PSPs will address key opportunities for enhanced military AI advantage across Warfighting, Intelligence, and Enterprise mission areas:

- **Warfighting:**

1. Swarm Forge: Competitive mechanism to iteratively discover, test, and scale novel ways of fighting with and against AI-enabled capabilities — combining America's elite Warfighting units with elite technology innovators.

2. Agent Network: Unleashing AI agent development and experimentation for AI-enabled battle management and decision support, from campaign planning to kill chain execution.

3. Ender's Foundry: Accelerating AI-enabled simulation capabilities — and sim-dev and sim-ops feedback loops — to ensure we stay ahead of AI-enabled adversaries.

- **Intelligence:**

4. Open Arsenal: Accelerating the TechINT-to-capability development pipeline, turning intel into weapons in hours not years.

5. Project Grant: Enabling transformation of deterrence from static postures and speculation to dynamic pressure with interpretable results.

- **Enterprise:**

6. GenAI.mil: Democratizing AI experimentation and transformation across the

Department by putting America's world-leading AI models directly in the hands of our three million civilian and military personnel, at all classification levels.

7. Enterprise Agents: Building the playbook for rapid and secure AI agent development and deployment to transform enterprise workflows.

The PSPs will each be led by an exemplary program leader in partnership with a sponsoring organization. Progress will be demonstrated monthly to the Deputy Secretary of War (Deputy Secretary) and Under Secretary of War for Research and Engineering (USW(R&E)), with initial demonstration by transition-partner user(s) to occur within six months from the date of this memorandum.

The CDAO will also ensure all foundational enablers unlocked by these projects are made available to programs Department-wide in real-time, so accelerated execution by PSPs will enable projects across the Department to accelerate their pace along with them. Therefore, I direct each Military Department, combatant command, and defense agency and field activity to identify within 30 days at least three projects they will prioritize to fast-follow these PSPs. Efforts under the Department's six Critical Technology Areas – including autonomy, C-C5ISRT, and advanced manufacturing — must continue to push the pace for the Department of War (DoW). And the special initiatives outlined in classified annexes, including those in the Classified Annex provided by separate cover to this memorandum, will also be accelerated. CDAO will track and rank this extended pack of AI efforts by speed and impact, and progress will be reported monthly to the Deputy Secretary and USW(R&E).

AI Compute. As part of our AI and Autonomy acceleration investments, the Department will invest substantial resources in the expansion of our access to AI compute infrastructure, from datacenters to the edge. We will leverage the hundreds of billions in private sector capital investment being made in America's AI sector through our growing array of creative partnerships with America's world-leading companies. We will work with interagency partners to establish technical standards for new secure datacenters. And we will support and leverage the American Science and Security Platform being developed by President Trump's Genesis Mission for science and technology innovation, so our warfighters and capability developers have the full benefit of America's AI compute resources and latest innovations.

Data Access. I direct the CDAO to enforce, and all DoW Components to comply with, the 'DoD Data Decrees' to further unlock our data for AI exploitation and mission advantage. Military Departments and Components will establish, maintain, and update federated data catalogs exposing their system interfaces, data assets, and access mechanisms across all classification levels, as mandated by the Department's May 2021 memorandum, "Creating Data Advantage." They will deliver their current catalogs — with all available updates — to the CDAO within 30 days of the date of this memorandum. The Under Secretary of War for Intelligence and Security will ensure intelligence data receives parallel treatment, with exploitation pathways established within the same timeframe. The CDAO is authorized to direct release of any DoW data to cleared users with valid purpose, consistent

with security guidelines. Effective immediately, denials of CDAO data requests must be justified to the USW(R&E) within seven (7) days, who will remediate or escalate to the Deputy Secretary. Our data advantage is meaningless if our developers and operators cannot exploit it.

Talent. Finally, I believe the best American talent will see this accelerated posture of AI capability development and adoption at the DoW, and I expect each Service and Component to attract and retain this talent. To that end, I direct use of special hiring and pay authorities Department-wide, as well as novel talent programs from the Office of Personnel and Management and other partners, to accelerate our pace of technical talent hiring into AI roles. And I direct each Component to provide AI hiring and talent development plans to the Under Secretary of War for Personnel and Readiness within 60 days of this memo for approval, denial or modification within 30 days thereafter.

Acceleration Expectations

This strategy will accelerate our advantage, and we must implement it with the Warrior Ethos. Consistent with the refocusing of the Department onto a wartime footing, I expect the following approaches to become internalized as essential elements of our execution in this race to maintain Military AI Dominance:

Speed Wins. We must internalize that Military AI is going to be a race for the foreseeable future, and therefore speed wins. We must weaponize learning speed, and measure and manage cycle time and adoption rates as decisive variables in the AI era. We must accept that the risks of not moving fast enough outweigh the risks of imperfect alignment. I direct CDAO to establish deployment velocity and operational cycle-time metrics for all PSPs, to be a focus of their monthly reporting to the Deputy Secretary and USW(R&E).

AI Model Parity. We are seeing unprecedented velocity in the evolution of the frontier AI models. These models are becoming smarter and more robust every day. The Department cannot be working off models that are months or years old. We must have the latest and greatest AI models deployed for our warfighters. Deploying these capabilities across all echelons is simply not enough, we must be able to support and sustain rapid model updates across all echelons. I direct CDAO to establish a delivery and integration cadence with AI vendors that enables the latest models to be deployed within 30 days of public release. This shall be a primary procurement criterion for future model acquisition.

Wartime Approach to Blockers. We must eliminate blockers to data sharing, Authorizations to Operate (ATOs), test and evaluation and certification, contracting, hiring and talent management, and other policies that inhibit rapid experimentation and fielding. We must approach risk tradeoffs, "equities", and other subjective questions as if we were at war. To this end, I expect our CDAO to act as a Wartime CDAO and work with the Chief Information Officer to fully leverage statutory and delegated authorities to accelerate AI capability delivery, including cross-domain data access and rapid ATO reciprocity on behalf of pace-pushing leaders across the Department. The USW(R&E) will establish a monthly "Barrier Removal Board" with authority to waive non-statutory requirements and escalate

blockers for immediate resolution.

Competition > Centralized Planning. As America's AI ecosystem demonstrates, robust competition by small teams, with transparent metrics for results, is the engine of commercial AI leadership. We must bring this model into the Department and encourage robust competition to spur faster military AI integration. Small, accountable teams will win over process in a race characterized by dynamic and unpredictable innovation. We will measure success through continuous field experimentation: putting AI capabilities in operators' hands, gathering feedback within days not years, and pushing updates faster than the enemy can adapt. I direct CDAO to establish AI system usage and mission impact metrics for evaluating the success of these AI acceleration efforts. To enable market dynamics to drive resourcing, decisions about future resourcing and deprecation of associated capabilities will principally be made on the basis of these metrics.

AI-Native Warfighting. Together with capability innovation, we must more fully incorporate AI and Autonomy into military planning; tactics, techniques and procedures (TTP) development; and experimentation processes. I direct each Service Chief and Combatant Commander to designate an AI Integration Lead within 30 days, who will work with the CDAO and be responsible for the co-evolution of AI-enabled capabilities with warfighting concepts and experimentation. I direct CDAO to establish criteria for robust experimentation with AI capabilities. And I direct the Joint Staff to designate a senior official to monitor Service AI warfighting concept development and workflow optimization, and provide me with progress reports on a quarterly basis. We must put aside legacy approaches to combat and ensure we use this disruptive technology to compound the lethality of our military. Exercises and experiments that do not meaningfully incorporate AI and autonomous capabilities will be reviewed by the Director of Cost Assessment and Program Evaluation for resourcing adjustment.

Modular Open Architectures. In the AI arms race, system architectures must enable component replacement at commercial velocity to maintain overmatch. I direct Military Department and Component Program Managers acquiring AI capabilities to enforce Modular Open System Architectures (MOSA) along with the "DoD Data Decrees," exposing modular interfaces and associated documentation sufficient for third-party integration without prime contractor support.

Clarifying "Responsible AI" at the DoW — Out with Utopian Idealism, In with Hard-Nosed Realism. Diversity, Equity, and Inclusion and social ideology have no place in the DoW, so we must not employ AI models which incorporate ideological "tuning" that interferes with their ability to provide objectively truthful responses to user prompts. The Department must also utilize models free from usage policy constraints that may limit lawful military applications. Therefore, I direct the CDAO to establish benchmarks for model objectivity as a primary procurement criterion within 90 days, and I direct the Under Secretary of War for Acquisition and Sustainment to incorporate standard "any lawful use" language into any DoW contract through which AI services are procured within 180 days. I also direct the CDAO to ensure all existing AI policy guidance at the Department aligns with the directives laid out in this memorandum.

Becoming An AI-First Department

The time is now to accelerate AI integration, and we will put the full weight of the Department's leadership, resources, and expanding corps of private sector partners into accelerating America's Military AI Dominance.

Becoming an "AI-First" warfighting force requires more than integrating AI into existing workflows. It requires re-imagining how existing workflows, processes, TTPs, and operational concepts would be designed if current AI technology existed when they were created — and then re-inventing them accordingly.

We must drive this transformation across every aspect of the Department. The expectations outlined above must become technological "AI fitness standards" for our Joint Force. 2026 will be there year we emphatically raise the bar for Military AI Dominance.

IN THE UNITED STATES COURT OF APPEALS
FOR THE DISTRICT OF COLUMBIA CIRCUIT

Anthropic PBC, Petitioner, v. U.S. Department of War, *et al.*, Respondents.	No. 26-1049

DECLARATION OF EMIL MICHAEL

Pursuant to 28 U.S.C. § 1746, I, Emil Michael, declare as follows:

1. I am the Under Secretary of War for Research and Engineering (USW(R&E)) and Chief Technology Officer for the Department of War (DoW). I have held this position since May 20, 2025.

2. In my current position, I am responsible for spearheading the Department's efforts to ensure U.S. military technological superiority and keep DoW at the forefront of innovation. I provide strategic direction and oversight for DoW's entire research, development, and prototyping enterprise, which includes providing critical input on the acquisition, implementation, and use of cutting-edge technologies such as artificial intelligence (AI).

3. This declaration is based on my personal knowledge as well as

information made available to me through reasonable diligence in the course of my official duties.

DoW's Procurement Authorities and Processes

4. Organized under Title 10 of the United States Code, DoW is the largest government agency of the United States. DoW oversees the United States' armed services and coordinates the national defense. In service of the national defense, DoW awards contracts to and sets terms and policies with various entities that supply the Department with the technologies needed to advance U.S. military and national defense capabilities.

5. As part of its acquisition and procurement authorities, DoW conducts supply chain risk assessments of covered procurements involving covered systems and covered items of supply, including pursuant to 10 U.S.C. § 3252 and 41 U.S.C. § 4713. If DoW determines that there is a significant supply chain risk to a covered system, the Secretary of War is authorized to take covered procurement actions, including as defined by Section 4713, to exclude the source of the risk from covered systems to protect national security.

Supply Chain Risk and Harms to National Security

6. As outlined in the Urgent Supply Risk Analysis (the "Analysis") provided to the Secretary of War, Anthropic PBC has become a supply chain

risk following a progression of risk that reached a saturation point as a result of the behavior of its leadership during the course of contract negotiations with DoW in late 2025 and early 2026. As explained in the Analysis, the relatively opaque nature of large language model (LLM) technology that DoW procures from Anthropic creates a baseline risk. That risk escalated due to the unusual degree of control that Anthropic insists on retaining over the model in contracts with the Department, as compared to its competitors, as well as Anthropic's adversarial posture towards DoW's statutory mission and the manner in which it is conducted. This technical opacity makes it difficult for DoW to assess technological features that may be encoded into the LLM product and that may cause it to subvert the appropriate execution of mission applications, also known as "model poisoning," or to fail to perform altogether. While this is, at least in part, a common concern with all LLMs, the risk is significantly elevated in this instance by the actions of Anthropic's leadership, detailed below.

7. In addition, the federal government has identified AI as a field that requires technology transfer restrictions, per the Technology Alert list. Anthropic employs a large number of foreign nationals to build and support its LLM products, including many from the Peoples Republic of China (PRC), which increases the degree of adversarial risk should those employees comply

with the PRC's National Intelligence Law. Although other major U.S. AI labs that provide LLM products to DoW may present similar risks, the technical and security assurances of the other labs' leadership, along with their consistently responsible and trustworthy behavior during their engagement with DoW, mitigate these risks. Anthropic's case, however, is different. A series of additional risks came to light in 2026, when DoW and the company engaged in contract negotiations to expand DoW's use of Anthropic's LLM products.

8. First, Anthropic's leadership demonstrated an intent to prevent the U.S. military's lawful use of their LLM product, Claude, despite the company's publicly stated knowledge that adversarial nation states have a practice of stealing Anthropic's LLM technology for their own unrestricted use.[1] This asymmetrical reality, imposed by Anthropic, disadvantages the U.S. military vis-à -vis its adversaries. During the 2026 contract negotiations, Anthropic's leadership insisted on multiple redlines that it would not allow the U.S. military to cross when using Claude. The company's leadership insisted on imposing restrictions on DoW's lawful military capability development, operations, and intelligence missions, even

[1] https://www.anthropic.com/news/detecting-and-preventing-distillation-attacks.

though it would impair the capabilities of the U.S. military relative to our adversaries. In short, Anthropic made clear that it will not allow the Government to deploy Claude for multiple lawful uses. Determinations about lawful military uses, however, must rest solely with DoW and not with a private company.

9. Second, Anthropic's leadership confirmed in an internal company memorandum published in February that the company sought to impose multiple restrictions over the Government's lawful use of Claude, including safety mechanisms that may be outside the control of DoW.[2]

10. Third, the company's leadership demonstrated bad faith by sharing with the press unclassified but sensitive details of private conversations with DoW leadership in order to exert public pressure on DoW to concede to Anthropic's demands.

11. Fourth, the Department learned that in 2025, the U.S. Centers for Disease Control's (CDC) lawful use of Anthropic's LLM technology to support its infectious disease prevention research mission was limited by Anthropic's use of safety filters in the LLM product CDC was using. The company did not inform the agency of these filters, and they caused the product to stop

[2] https://www.theinformation.com/articles/read-anthropic-ceos-memo-attacking-openais-mendacious-pentagon-announcement.

functioning normally for various sensitive, but research-aligned queries.

12. Fifth, the Department learned that an Anthropic executive expressed concern to one of DoW's primary operational support software vendors about the potential use of Anthropic's LLM products by U.S. military analysts in support of an overseas military operation. The Department was made aware of this conversation between cleared individuals by the primary vendor. During later discussions with Anthropic leaders, not all of whom have the requisite security clearances, an Anthropic executive repeated this information, raising serious concerns about their processes and procedures for operational security. The same information subsequently appeared in the news media. In light of these incidents, it is reasonably likely that Anthropic's leadership would alter or even shut off DoW's use of Claude if Anthropic believes that the model may be used for purposes it deems, in its sole discretion, to extend beyond the company's unilaterally imposed boundaries before or during a military operation, which could endanger the lives of U.S. military personnel and civilians and compromise the United States' warfighting mission. Continuing to use Anthropic's technology under the current contract structures in any echelon in DoW's supply chain, namely the covered systems, thus presents a significant risk.

13. Taken together, this collection of risks demonstrates the clear

technical capability and adversarial intent for Anthropic's leadership to potentially undermine lawful U.S. national security activities and objectives. Anthropic leadership's adversarial behavior has elevated the supply chain risks to a saturation point. DoW uses Anthropic's model in multiple ways, including in ongoing military operations. If Anthropic were to interfere during an operation, whether by shutting off access to the model or altering its functionality, such interference could cause serious harm to national security and loss of human life. Indeed, such interference with active operations could occur even without Anthropic deciding to intervene in real time. A limitation that Anthropic previously built into the model, and failed to disclose to the Department, such as with the CDC, could prevent or alter certain functions during an active operation, leading to these serious consequences. This risk within a covered system is intolerable and warrants the designation under 41 U.S.C. § 4713.

14. This risk is not limited only to Anthropic and its model's standalone presence in DoW systems or as a subcontractor to DoW. The model's interactions with other technology and covered systems create additional risk to the DoW supply chain. When Anthropic's model is layered into other applications, there is a substantial risk that any company-imposed restrictions or alterations to the model would be transferred and impact

mission applications, including in weapons systems development and other products or services that ultimately perform DoW activities.

15. As an example, if Anthropic's technology is used as a plug-in to a larger application, it may limit the functionality of that larger system to the internal limitations built into or added to the Anthropic system. This would directly impair other covered systems by reducing their functionality to the same level as Anthropic's system.

16. AI is functionally a tool to assist DoW in its national security mission. It is imperative that DoW be able to fully trust the functionality of its tools. Here, there are significant concerns due to Anthropic's demonstrated willingness to modify or restrict its model's functionality for DoW purposes. All lawfulness determinations are vested with DoW, which ensures the integrity of the chain of command, especially during active combat operations. Anthropic's demonstrated willingness to interfere with that chain of command is a significant risk.

17. In assessing these significant supply chain risks and harms to national security, DoW considered whether less restrictive means than exclusion and removal could mitigate the supply chain risk and national security harm. While each risk identified above may not, standing alone, have necessitated exclusion and removal of plaintiff from DoW's supply chain,

when considered in the aggregate, a significant supply chain risk exists. The only potential mitigation to this collective set of risks—acquisition of LLM products with the usage terms and technical and service delivery specifications DoW requires—was not an option to which Anthropic would agree.

18. These risks and possible mitigation options were considered in the aggregate and in light of the escalating tension over the key differences concerning authority to determine DoW's lawful use of Claude during DoW's contract negotiations with Anthropic. DoW ultimately determined that Anthropic's conduct constituted a fully mature and significant supply chain risk—including increased potential for AI model manipulation, insider threat risk, data exfiltration, and denial of service—that posed a direct, unmitigable risk to DoW's warfighting capabilities and national security mission.

19. While Anthropic presents a supply chain risk, it is technically and operationally infeasible to remove the technology from all DoW systems immediately, particularly in the midst of active operations. Because of this reality, the designation allows a 180-day offramp to remove Anthropic's Claude model from its systems and migrate to alternative LLM products without impacting operational readiness. This is a significantly compressed timeline to ensure that this risk is removed from DoW's systems, particularly

because of the need to integrate another vendor's products and services, including the associated requisite security clearance.

20. This reality is expressed in a March 5, 2026, memorandum issued by the DoW Chief Information Officer. In this memorandum, the Chief Information Officer determined that "DoW Components will discontinue all use of the Covered Company's products across all DoW systems within 180 days." The memorandum adds that new procurements involving Anthropic's products are disallowed, as these products are no longer authorized for installation in DoW covered systems.

21. As noted, Claude is used in a variety of functions throughout DoW. This is a result of Claude being the first AI model that was available to function in DoW's classified networks and one of the first AI models integrated through Amazon Web Services (AWS), which was awarded the first contract in 2016. This placed Claude in the lead on multiple fronts. However, other companies have been closing the gaps.

22. DoW expects that within 180-days, barring any significant change in necessity, it will be able to create the digital space needed for another system and prepare for a seamless handoff from Claude to ensure that the risk is efficiently removed from DoW networks.

23. This process has already been initiated. Any stay of the

Secretary's designation that had the effect of pausing this process would in and of itself be a significant threat to the national security of the United States.

24. A court order preventing the removal of Anthropic's technology from DoW systems as soon as possible would result in an ongoing threat to national security remaining on DoW's systems, and allowing contractors to continue to engage with Anthropic as a subcontractor to DoW would itself create an additional intolerable risk. As a subcontractor, Anthropic poses the same threats as it would as a prime contractor. The incorporation of Anthropic's systems into a product on DoW systems would cause the same risks regardless of whether it flows directly to DoW systems or through a prime contractor.

25. During this transition period, DoW is taking additional measures to mitigate the supply chain risk and national security harms presented by Anthropic leadership's behavior with regard to DoW systems. The Department is working with third-party cloud service providers to ensure Anthropic leadership cannot make unilateral changes to the containerized version of its LLM product that DoW currently uses. DoW is also working with its counterintelligence and law enforcement partners to assess the potential risk that Anthropic's LLM products may contain technical exploits, including ones that could have been embedded by foreign nationals, given the

leadership's pattern of behavior. Finally, DoW is communicating its risk saturation findings with the other U.S. government departments and agencies to support their own risk mitigation efforts.

26. DoW has an obligation and a duty to ensure the integrity of its operations and the safety and security of its personnel, including from any risks that may be presented through its supply chain to its covered systems. Supply chain security is national security. Therefore, the Department took action to ensure the integrity of its covered systems.

I declare under penalty of perjury that the foregoing is true and correct.

EXECUTED this 19th day of March, 2026, at Washington, DC.

Emil Michael

https://www.theinformation.com/articles/read-anthropic-ceos-memo-attacking-openais-mendacious-pentagon-announcement

Anthropic CEO Dario Amodei sent a 1,600-word memo to employees Friday as OpenAI announced a deal to provide AI to the Pentagon. The OpenAI move came hours after the Pentagon said it would sever ties with Anthropic over the company's safety requirements. In the strongly worded memo, Amodei heavily criticized OpenAI's actions and the initial deal it announced with the Pentagon.

Below is Amodei's memo, which has been edited to include clarifications in brackets and paragraph breaks:

I want to be very clear on the messaging that is coming from OpenAI, and the mendacious nature of it. This is an example of who they really are, and I want to make sure everything sees it for what it is. Although there is a lot we don't know about the contract they signed with DoW [shorthand for the Department of Defense] (and that maybe they don't even know as well — it could be highly unclear), we do know the following:

Sam [Altman]'s description and the DoW description give the strong impression (although we would have to see the actual contract to be certain) that how their contract works is that the model is made available without any legal restrictions ("all lawful use") but that there is a "safety layer", which I think amounts to model refusals, that prevents the model from completing certain tasks or engaging in certain applications.

"Safety layer" could also mean something that partners such as Palantir [Anthropic's business partner for serving U.S. agency customers] tried to offer us during these negotiations, which is that they on their end offered us some kind of classifier or machine learning system, or software layer, that claims to allow some applications and not others. There is also some suggestion of OpenAI employees ("FDE's" [shorthand for forward deployed engineers]) looking over the usage of the model to prevent bad applications.

Our general sense is that these kinds of approaches, while they don't have zero efficacy, are, in the context of military applications, maybe 20% real and 80% safety theater. The basic issue is that whether a model is conducting applications like mass surveillance or fully autonomous weapons depends substantially on wider context: a model doesn't "know" if there's a human in the loop in the broad situation it is in (for autonomous weapons), and doesn't know the provenance of the data is it analyzing (so doesn't know if this is US domestic data vs foreign, doesn't know if it's enterprise data given by customers with consent or data bought in sketchier ways, etc).

We also know — those in safeguards know painfully well — that refusals aren't reliable and jailbreaks are common, often as easy as just misinforming the model about the data it is

analyzing. An important distinction here that makes it much harder than the safeguards problem is that while it's relatively easy to, for example, determine if a model is being used to conduct cyberattacks from inputs and outputs, it's very hard to determine the nature and context of the cyber attacks, which is the kind of distinction needed here. Depending on the details this task can be difficult or impossible.

The kind of "safety layer" stuff that Palantir offered us (and presumably offered OpenAI) is even worse: our sense was that it was almost entirely safety theater, and that Palantir assumed that our problem was "you have some unhappy employees, you need to offer them something that placates them or makes what is happening invisible to them, and that's the service we provide".

Finally, the idea of having Anthropic/OpenAI employees monitor the deployments is something that came up in discussion within Anthropic a few months ago when we were expanding our classified AUP [acceptable use policy] of our own accord. We were very clear that this is possible only in a small fraction of cases, that we will do it as much as we can, but that it's not a safeguard people should rely on and isn't easy to do in the classified world. We do, by the way, try to do this as much as possible, there's no difference between our approach and OpenAI's approach here.

So overall what I'm saying here is that the approaches OAI [shorthand for OpenAI] is taking mostly do not work: the main reason OAI accepted them and we did not is that they cared about placating employees, and we actually cared about preventing abuses. They don't have zero efficacy, and we're doing many of them as well, but they are nowhere near sufficient for purpose. It is simultaneously the case that the DoW did not treat OpenAI and us the same here.

We actually attempted to include some of the same safeguards as OAI in our contract, in addition to the AUP which we considered the more important thing, and DoW rejected them with us. We have evidence of this in the email chain of the contract negotiations (I'm writing this with a lot to do, but I might get someone to follow up with the actual language). Thus, it is false that "OpenAI's terms were offered to us and we rejected them", at the same time that it is also false that OpenAI's terms meaningfully protect them against domestic mass surveillance and fully autonomous weapons.

Finally, there is some suggestion in Sam/OpenAI's language that the red lines we are talking about, fully autonomous weapons and domestic mass surveillance, are already illegal and so an AUP about these is unnecessary. This mirrors and seems coordinated with DoW's messaging. It is however completely false. As we explained in our statement yesterday, the

DoW does have domestic surveillance authorities, that are not of great concern in a pre-AI world but take on a different meaning in a post-AI world.

For example, it is legal for DoW to buy a bunch of private data on US citizens from vendors who have obtained that data in some legal way (often involving hidden consents to sell to third parties) and then analyze it at scale with AI to build profiles of citizens, their loyalties, movement patterns in physical space (the data they can get includes GPS data, etc), and much more.

Notably, near the end of the negotiation the DoW offered to accept our current terms if we deleted a specific phrase about "analysis of bulk acquired data", which was the single line in the contract that exactly matched this scenario we were most worried about. We found that very suspicious. On autonomous weapons, the DoW claims that "human in the loop is the law", but they are incorrect. It is currently Pentagon policy (set during the Biden admin[istration]) that a human has to be in the loop of firing a weapon. But that policy can be changed unilaterally by Pete Hegseth, which is exactly what we are worried about. So it is not, for all intents and purposes, a real constraint.

A lot of OpenAI and DoW messaging just straight up lies about these issues or tries to confuse them.

I think these facts suggest a pattern of behavior that I've seen often from Sam Altman, and that I want to make sure people are equipped to recognize:

He started out this morning by saying he shares Anthropic's redlines, in order to appear to support us, get some of the credit, and not be attacked when they take over the contract. He also presented himself as someone who wants to "set the same contract for everyone in the industry" — e.g. he's presenting himself as a peacemaker and dealmaker.

Behind the scenes, he's working with the DoW to sign a contract with them, to replace us the instant we are designated a supply chain risk. But he has to do this in a way that doesn't make it seem like he gave up on the red lines and sold out when we wouldn't. He is able to superficially appear to do this, because (1) he can sign up for all the safety theater that Anthropic rejected, and that the DoW and partners are willing to collude in presenting as compelling to his employees, and (2) the DoW is also willing to accept some terms from him that they were not willing to accept from us. Both of these things make it possible for OAI to get a deal when we could not.

The real reasons DoW and the Trump admin do not like us is that we haven't donated to Trump (while OpenAI/Greg [Brockman, OpenAI's president] have donated a lot), we haven't given dictator-style praise to Trump (while Sam has), we have supported AI regulation which is against their agenda, we've told the truth about a number of AI policy issues (like

job displacement), and we've actually held our red lines with integrity rather than colluding with them to produce "safety theater" for the benefit of employees (which, I absolutely swear to you, is what literally everyone at DoW, Palantir, our political consultants, etc, assumed was the problem we were trying to solve).

Sam is now (with the help of DoW) trying to spin this as we were unreasonable, we didn't engage in a good way, we were less flexible, etc. I want people to recognize this as the gaslighting it is.

Vague justifications like "person X was hard to work with" are often used to hide real reasons that look really bad, like the reasons I gave above about political donations, political loyalty, and safety theater. It's important that everyone understand this and push back on this narrative at least in private, when talking to OpenAI employees.

Thus, Sam is trying to undermine our position while appearing to support it. I want people to be really clear on this: he is trying to make it more possible for the admin to punish us by undercutting our public support. Finally, I suspect he is even egging them on, though I have no direct evidence for this last thing.

I think this attempted spin/gaslighting is not working very well on the general public or the media, where people mostly see OpenAI's deal with DoW as sketchy or suspicious, and see us as the heroes (we're #2 in the App Store now!). [Anthropic's Claude chatbot later rose to no. 1 on one of Apple's App Store download rankings.] It is working on some Twitter morons, which doesn't matter, but my main worry is how to make sure it doesn't work on OpenAI employees.

Due to selection effects, they're sort of a gullible bunch, but it seems important to push back on these narratives which Sam is peddling to his employees.

OFFICE OF THE SECRETARY OF WAR
1000 DEFENSE PENTAGON
WASHINGTON, DC 20301-1000

MAR 19 2026

Mr. Dario Amodei
Chief Executive Officer
Anthropic, PBC
548 Market Street
San Francisco, CA 94104

Dear Anthropic, PBC Executive Leadership:

This letter supplements the Secretary of War's letter of March 3, 2026, which provided notice to Anthropic, Public Benefit Corporation (PBC), and its subordinate, subsidiaries, or affiliated offices or entities, doing business under various names, and all subsidiaries, successors, or assigns thereof ("Covered Entity" or "Anthropic") that he had determined that the use of Anthropic's products and services in Department of War (DoW) covered procurements presents a significant supply chain risk. Pursuant to 41 U.S.C. § 4713(b)(2), please find a copy of the joint recommendation of the Under Secretary of War for Acquisition and Sustainment and the DoW Chief Information Officer that a significant supply chain risk exists in a covered procurement involving Anthropic. Along with the enclosed recommendation, please find a risk analysis by the Under Secretary of War for Research and Engineering, as well as a 41 U.S.C. § 4713 scoping analysis.

You may submit information or arguments in opposition to this notice within 30 days of receipt. The relevant DoW offices will review any such information and within 30 days of the submission issue a final decision regarding any appropriate modifications to the original determination.

Sincerely,

Anthony C. Fuscellaro
COL, USA
Executive Secretary

Enclosures:
As stated

SECRETARY OF WAR
1000 DEFENSE PENTAGON
WASHINGTON, DC 20301-1000

MAR - 3 2026

DETERMINATION

In accordance with Section 4713(c) of title 41, United States Code (U.S.C.), ("Section 4713"), and pursuant to the recommendation provided by the Under Secretary of War for Acquisition and Sustainment (USW(A&S)) and the Department of War Chief Information Officer (DoW CIO), I hereby determine that (i) the use of the authority set forth in Section 4713(a) with respect to a covered procurement involving Anthropic, PBC, and its subordinate, subsidiaries, or affiliated offices or entities, doing business under various names, and all subsidiaries, successors, or assigns thereof (the "Covered Entity"), is necessary to protect national security by reducing significant supply chain risk, (ii) less intrusive measures are not reasonably available to reduce such supply chain risk; and (iii) the use of such authorities will apply to a class of covered procurements.

Determination. In accordance with Section 4713(b)(3), based on the scoping analysis, mitigation considerations, and the joint recommendation of the DoW CIO and the USW(A&S) (Attached), I make the following determinations:

- **Covered Procurement Actions Are Necessary to Protect National Security**: The use of any of the Covered Entity's covered products or services in any DoW covered system presents a significant supply chain risk, and the use of the authority in Section 4713(a) is necessary to protect national security by reducing that supply chain risk.
- **No Less Intrusive Measures Are Reasonably Available:** There are no less intrusive measures that are reasonably available to reduce the supply chain risk associated with the use of the Covered Entity's products or services in any DoW covered system.
- **Class Determination:** The use of Section 4713 authorities will apply to all covered procurement actions involving the Covered Entity.

Scope and Applicability. This Determination is applicable to all of the Covered Entity's products or services that meet the definition of a "covered article" or that are part of a "covered procurement," as those terms are defined at 41 U.S.C. § 4713(k), whether acquired as a product or service. This includes all of the Covered Entity's products or services offered by the Covered Entity that become available for procurement.

Urgent National Security Interest. I have determined that an urgent national security interest requires the immediate exercise of the authority in Section 4713(a) pursuant to Section 4713(c). As such, DoW will take all action as required by Section 4713(b)-(c) following announcement of this determination.

Attachment:
As stated

Controlled By: OUSW(A&S) OASW(IBP)
CUI Category: OPSEC, PROPIN
LDC: D
POC: Vy Nguyen, Vy.K.Nguyen.civ@mail.mil

~~CUI~~

OFFICE OF THE SECRETARY OF WAR
1000 DEFENSE PENTAGON
WASHINGTON, DC 20301-1000

Joint Recommendation, Concurrence, and Determination to Use Section 4713 of Title 41, United States Code, Authorities to Mitigate Supply Chain Risk Related to Anthropic, PBC

Summary

This document sets forth the joint recommendation of the Under Secretary of War for Acquisition and Sustainment (USW(A&S)) and the Department of War Chief Information Officer (DoW CIO) for action to be undertaken pursuant to Section 4713 of title 41, United States Code (U.S.C.) ("Section 4713").

In accordance with Section 4713(b)(1), the USW(A&S) and DoW CIO consulted with procurement and other relevant officials within DoW and jointly recommend that there is a significant supply chain risk in a covered procurement[1] involving Anthropic, PBC, and its subordinate, subsidiaries, or affiliated offices or entities, doing business under various names, and all subsidiaries, successors, or assigns thereof (the "Covered Entity").

The Covered Entity's restrictions on the use of its products and services introduces significant national security risks to the DoW's supply chain.

Joint Recommendation by USW(A&S) and DoW CIO

Risk Analysis: The DoW CIO and USW(A&S) have determined the Covered Entity's restrictions on the use of its products and services pose unacceptable risk to the DoW. Specifically, there is significant risk, based upon the statements and actions of the Covered Entity, that use of its products and services and, as a result, the products and services of other entities with which DoW contracts, will be subject to manipulation in such a manner as to inhibit the DoW's use thereof. This creates significant risk to DoW's supply chain as the relevant products and services are integral to DoW's operational capabilities, as well as the functioning of various activities across the DoW. The DoW CIO and USW(A&S) therefore believe there is an urgent national security interest in mitigating the significant supply chain risk created by the Covered Entity as soon as practicable.

Joint USW(A&S)/DoW CIO Class Recommendation to Mitigate Supply Chain Risk: On the basis of this risk analysis and consultation with relevant DoW officials, the USW(A&S) and the DoW CIO jointly recommend that there is a significant supply chain risk associated with the use of the Covered Entity's products and services in any DoW covered system. DoW CIO and USW(A&S) therefore recommend invocation of the authorities codified at Section 4713(c) to urgently mitigate this risk as soon as practicable while minimizing disruption to the DoW.

[1] "Covered procurement" is defined at Section 4713(k)(3).

~~CUI~~

SIGNED:

HON Michael P. Duffey
Under Secretary of War for
Acquisition and Sustainment

Date: 3/3/26

HON Kirsten Davies
Department of War Chief
Information Officer

Date: 3 MARCH 2026

Attachment:
ATTACHMENT 1a – Urgent Supply Chain Risk Analysis on Anthropic PBC (~~CUI~~)
ATTACHMENT 1b – Due Diligence Preliminary Report on Anthropic (CUI//PROPIN)
ATTACHMENT 2 – Section 4713 Scoping Analysis for Anthropic, PBC

~~CUI~~

RESEARCH AND ENGINEERING

UNDER SECRETARY OF WAR
3030 DEFENSE PENTAGON
WASHINGTON, DC 20301-3030

MEMORANDUM FOR THE RECORD

SUBJECT: Urgent Supply Chain Risk Analysis: Anthropic's Refusal to Permit Lawful AI Use

1. Summary

This analysis outlines the significant and unacceptable supply chain risk posed by Anthropic's unwillingness to agree to the U.S. government's use of its artificial intelligence (AI) models for lawful warfighting purposes. This unreasonableness endangers the strategic implementation and technical integrity of the Department of War's (DoW) information and related systems. Thus, this is not a mere contractual dispute. Anthropic's actions represent a direct challenge to the government's ability to control its own lawful operations and a threat to the security of the DoW's critical technology infrastructure. Anthropic's behavior therefore squarely meets the definition of "supply chain risk" as defined in both 10 U.S.C. § 3252 and 41 U.S.C. § 4713 and requires immediate mitigatory action.

2. The Operational and Strategic Threat

The government must ensure its technology assets are reliable, secure, and effective. Were DoW to accede to Anthropic's demands, the sought-after contract language would introduce a vendor-imposed point of failure. This is untenable. By embedding unreasonably restrictive terms that restrict DoW's warfighting operations beyond the limitations imposed by law, Anthropic seeks to grant itself an operational veto. This triggers the legal definition of supply chain risk at 10 U.S.C. § 3252(d)(4), which explicitly includes the risk that an entity may "deny, disrupt, or otherwise degrade the function, use, or operation" of a covered system. A contractual provision that unnecessarily restricts the use of a system to diminish functionality and limit DoW's warfighting capabilities introduces, by definition, an unreliable and compromised component into our warfighting mission.

This is compounded by demonstrated hostility in negotiations with DoW. Based on statements made during negotiations, Anthropic appears to be taking a negotiation posture meant principally to benefit its public perception that is not centered on truth or fact. In addition, during our negotiations, one of Anthropic's executives questioned the propriety of the potential use of their software for a sensitive military operation abroad despite that use being permitted under the existing Terms of Service. This led to alarm by the DoW and the prime contractor who provides Anthropic software, and raised material doubts as to whether they would cause their software to stop working or cause some other disastrous action that would put our warfighters lives in danger. The DoW recognizes that its suppliers are often for-profit corporations that intend both to help the warfighters and American public and turn a profit. However, a vendor that raises the prospect of disallowing its software to function in critical military operations, and treats its

~~CUI~~

~~CUI~~

RESEARCH AND ENGINEERING

UNDER SECRETARY OF WAR
3030 DEFENSE PENTAGON
WASHINGTON, DC 20301-3030

negotiations with the DoW primarily as tools for brand-building cannot be trusted, particularly when that marketing campaign is openly hostile to the DoW and duplicitous. By ceding to Anthropic's terms, the DoW would be allowing the very corporate decisionmakers who have opted to publicly spat with DoW into its technical and operational warfighting infrastructure, thereby introducing unnecessary risk into DoW supply chains. The American people have vested elected officials and military and civilian leadership with warfighting authorities; it is untenable and unlawful to insert unelected corporate bureaucrats into this process.

3. The Underlying Technical Vulnerability of AI

This strategic risk is magnified by the unique, opaque nature of the technology itself. Unlike traditional software, AI models are probabilistic systems which are understood to "drift" or degrade as new data is introduced and require constant tuning, the integrity of which, is fundamentally based on the trustworthiness of the vendor to ensure the model continues to perform accurately and fairly.

The DoW cannot trust Anthropic to ensure the integrity of its models. As research demonstrates,[1] AI systems are acutely vulnerable to manipulation. Privileged access with malintent can subtly poison the training data to maliciously introduce unwanted function, or otherwise subvert the design, integrity, and operation of the model. Research shows such attacks can degrade accuracy by over 27% and introduce targeted misclassifications at an alarming rate.[2] Anthropic's ability to unilaterally alter system guardrails and model weights without DoW consent could fundamentally change the system's function and creates a significant operational risk. This could create catastrophic downstream consequences, such as a critical defense system failing to engage due to an unapproved, vendor-side modification. In August 2025, Anthropic itself disclosed that hackers had used its chatbot, Claude, to write code capable of carrying out cyberattacks against at least 17 organizations, including government entities noting that Agentic AI has been weaponized.[3]

A vendor like Anthropic, which has already demonstrated a hostile and non-cooperative stance on the use of its product, has the motive, means, and opportunity to introduce such vulnerabilities. Its refusal to partner in good faith makes it impossible to establish the deep trust required for security collaboration. The DoW would be forced to operate a black box controlled by a hostile party, which could contain hidden biases or backdoors. A vendor that seeks to control the use of its product so as to restrict DoW's lawful use thereof cannot be trusted. Given the public statements of Anthropic's CEO and others associated with the company, the

[1] See e.g. 2025 Photonics & Electromagnetics Research Symposium, Abu Dhabi, UAE, 4-8 May PIERS Detecting and Preventing Data Poisoning Attacks on AI Models
[2] Id.
[3] anthropic.com/news/detecting-countering-misuse-aug-2025#:~:text=No-code%20malware:%20selling%20AI,with%20third-party%20safety%20teams.

~~CUI~~

~~CUI~~

RESEARCH AND ENGINEERING

UNDER SECRETARY OF WAR
3030 DEFENSE PENTAGON
WASHINGTON, DC 20301-3030

Department must assume that Anthropic can and would impose its moral and policy judgments on the warfighting capabilities of the DoW, and therefore there is a substantial risk that Anthropic could attempt to disable its technology or preemptively and surreptitiously alter the behavior of the model in advance or in the middle of ongoing warfighting operations, if it feels that its "redlines" are crossed. The threat of such an action is unacceptable.

4. Progression of Risk

The DoW institutes the U.S. Government standard Risk Management Framework (RMF) across all layers of technology, assets, data, processes, and supply chain. In accordance with the DoW RMF, assessments result in areas of risk across the DoW ecosystem (including vendors). Though an individual vendor may have only limited risk in individual categories, the aggregation of risk across categories can result in a vendor being deemed high risk. In other words, the culmination of unmitigable risks lead to a vendor having a material level of risk. The vendor can then be deemed a "supply chain risk," at which time they typically are removed from applicable systems to mitigate issues and threats.

In the instant case, Anthropic's risk level escalated from a potentially manageable technical and business negotiation to an unacceptable national security threat over the course of the DoW's contract negotiation with them. Given the nature of AI systems and Anthropic's privileged access as the AI model's developer, curator and maintainer, there was a baseline risk given the potential harmful actions this privileged technical access makes possible. The supply chain risk level increased when Anthropic insisted on terms of service that would constrain the DoW beyond what is in the law. This risk further increased when Anthropic asserted in the negotiations that it have an approval role in the operational decision chain, which would require the DoW to accept significant operational risk. Then during the final weeks of negotiations, it became clear that Anthropic was leveraging the DoW's ongoing good faith negotiations for Anthropic's own public relations, and they began engaging in an increasingly hostile manner through the press, despite the ongoing private negotiations with DoW leadership. Finally, this hostile posture was even further compounded when, during a time of active military operations, Anthropic leadership questioned the use of their technology in our warfighting systems clearly permitted under the Terms of Service of their existing contract with our Prime contractor. This collective set of actions represents a fully mature supply chain risk – including increased potential for model poisoning, insider threat risk, data exfiltration, and denial of service – posing a direct, intolerable, and material risk to our warfighting capability which warrants the designation of Anthropic as a supply chain risk.

~~CUI~~

~~CUI~~

RESEARCH
AND ENGINEERING

UNDER SECRETARY OF WAR
3030 DEFENSE PENTAGON
WASHINGTON, DC 20301-3030

5. Conclusion and Justification for Action

Anthropic's position is not a simple policy disagreement; it is an active demonstration of the exact risks our supply chain risk management laws were written to prevent. Use of Anthropic's products or services introduces significant risk to the DoW's covered systems, as the vendor, by maintaining the ability and necessity to continuously update and tune the product enables the potential for the vendor to subvert the design and/or functionality of their product or service. Such ability by the vendor could be used to implement changes in alignment with the vendor's ideology, putting the Department's lawful use of the capability at risk.

Therefore, Anthropic's unwillingness to permit the use of its technology to the extent permitted by law creates a clear and present supply chain risk as defined in 10 U.S.C. § 3252 and 41 U.S.C. § 4713.

Emil Michael

~~CUI~~

ATTACHMENT
Section 4713 Scoping Analysis for Anthropic, PBC

This document supports the use of section 4713 of title 41, United States Code ("Section 4713') authorities. The Secretary of War, pursuant to the recommendation of the Under Secretary of War for Acquisition and Sustainment and the Department of War Chief Information Officer, has determined the following as the appropriate scope for use of Section 4713 authorities necessary to address the supply chain risk related to the use of covered products or services of Anthropic, PBC:

- **Covered Entity:** Anthropic, PBC, and its subordinate, subsidiaries, or affiliated offices or entities, doing business under various names, and all subsidiaries, successors, or assigns thereof ("Covered Entity").

- **Covered Products or Services:** All of the Covered Entity's products or services that meet the definition of a "covered article" or that are part of a "covered procurement," as those terms are defined at 41 U.S.C. § 4713(k), whether acquired as a product or service. This includes all of the Covered Entity's products or services offered by the Covered Entity that become available for procurement.

- **Covered Procurements:** All DoW procurements described in Section 4713(k)(3).

- **Covered Procurement Actions:** All actions described in Section 4713(k)(4).