UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

ANTHROPIC PBC, Plaintiff, v. U.S. DEPARTMENT OF WAR, *et al.*, Defendants.	Case No. 3:26-cv-01996-RFL **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 Title 10, Section 3252 Authorities

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 under 10 U.S.C. § 3252, DoW conducts supply chain risk assessments of covered procurements involving covered systems and covered items of supply, as defined in that section. 10 U.S.C. § 3252(d)(3), (4). 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, as defined by Section 3252, to exclude the source of the risk from covered systems to protect national security.

6. Under Section 3252's implementing regulations, this exclusion authority may be exercised by the Secretary of War only after "[o]btaining a joint recommendation by the Under Secretary of War for Acquisition and Sustainment and the Chief Information Officer of the Department of War, on the basis of a risk assessment by the Under Secretary of War for Intelligence, that there is a significant supply chain risk to a covered system." 48 C.F.R. § 239.7304. The Office of the Under Secretary of War for Intelligence and Security[1] (USW(I&S)) ordinarily would have had responsibility for conducting such supply chain risk assessments because of its general expertise in handling security matters and its prior relationships with the information offices of the Department, including the Office of the Chief Information Officer, which reported to USW(I&S) until 2012. But after a recent reorganization within DoW, the subject matter expertise for conducting certain risk assessments is no longer located solely within USW(I&S).

DoW's 2025 Reorganization

7. Prior to 2025, the Chief Digital and Artificial Intelligence Office (CDAO), founded in 2022, was a standalone function that reported directly to the Deputy Secretary of War. CDAO's mission is to accelerate DoW's adoption of AI to ensure that our warfighters have the best capabilities to dominate on the battlefield and have full trust that the technologies they are using to create decision advantage are secure and trustworthy.

8. In 2025, DoW underwent a reorganization. As part of the reorganization, CDAO was realigned and began to report to the Under Secretary of War for Research and Engineering. Because of its institutional and subject matter expertise, CDAO inherited responsibility for Section 3252 supply

[1] In the FY 2020 NDAA, the Under Secretary for Intelligence was renamed as the Under Secretary for Intelligence and Security to better capture the scope of the authorities vested in the office.

chain risk assessments relating to AI issues. As a result, my office has assumed responsibility for providing CDAO's supply chain risk assessments relating to AI issues to the Under Secretary of War for Acquisition and Sustainment and the Chief Information Officer in accordance with 48 C.F.R. § 249.7304. In addition to CDAO possessing the relevant authorities, CDAO and my office are DoW's subject matter experts for AI issues and are therefore best able to provide the comprehensive risk assessment that informs the determinations under Section 3252. As appropriate, my office and CDAO also coordinate AI risk assessments with the Chief Information Officer.

Supply Chain Risk and Harms to National Security

9. 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 retains over the model, 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.

10. 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.

11. 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.[2] 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 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.

12. 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.[3]

13. 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.

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

[2] https://www.anthropic.com/news/detecting-and-preventing-distillation-attacks.
[3] https://www.theinformation.com/articles/read-anthropic-ceos-memo-attacking-openais-mendacious-pentagon-announcement.

15. Fifth, the Department learned that during an active overseas military operation, 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 during the 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.

16. 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. This risk within a covered system is intolerable and warrants the designation under 10 U.S.C. § 3252.

17. 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.

18. 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.

19. 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.

20. 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.

21. 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.

22. 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.

23. 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.

24. 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.

25. 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.

26. This process has already been initiated. An injunction pausing this process would in and of itself be a significant threat to the national security of the United States.

27. An injunction 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.

28. 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.

29. 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 17th day of March, 2026, at Washington, DC.

Emil Michael