EXHIBIT 1

Elisabeth S. Theodore*
elisabeth.theodore@arnoldporter.com
Benjamin C. Mizer*
benjamin.mizer@arnoldporter.com
Eun Young Choi*
eunyoung.choi@arnoldporter.com
Samuel F. Callahan*
sam.callahan@arnoldporter.com
Aaron X. Sobel*
aaron.sobel@arnoldporter.com
ARNOLD & PORTER KAYE SCHOLER LLP
601 Massachusetts Ave. NW
Washington, District of Columbia 20001
Telephone: (202) 942-5000
Facsimile: (202) 942-5999

Allyson Myers (SBN 342038)
ally.myers@arnoldporter.com
ARNOLD & PORTER KAYE SCHOLER LLP
777 S. Figueroa St. 44th Floor
Los Angeles, CA 90017
Telephone: (213) 243-4000
Facsimile: (213) 243-4199

Attorneys for Amicus Curiae Alan Z. Rozenshtein

*Application for admission *pro hac vice* forthcoming

IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

ANTHROPIC PBC,

Plaintiff,

v.

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

Defendants.

Case No. 3:26-cv-01996-RFL

[PROPOSED] BRIEF OF AMICUS CURIAE ALAN Z. ROZENSHTEIN IN SUPPORT OF PLAINTIFF'S MOTION FOR A TEMPORARY RESTRAINING ORDER, PRELIMINARY INJUNCTION, OR SECTION 705 STAY

Date: March 24, 2026
Time: 1:30 P.M.
Judge: Hon. Rita F. Lin
Crtrm.: 15, 18th Floor

Complaint filed: March 9, 2026

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes and Regulations

Other Authorities

INTRODUCTION AND INTEREST OF AMICUS CURIAE

Professor Alan Z. Rozenshtein is a tenured Associate Professor of Law at the University of Minnesota Law School. He is the Research Director and a Senior Editor at Lawfare, a Nonresident Senior Fellow at the Brookings Institution, a Visiting Senior Fellow at the Institute for Law & AI, and a Term Member of the Council on Foreign Relations. For over two years, he worked as an Attorney Advisor in the National Security Division of the U.S. Department of Justice. Professor Rozenshtein's research and teaching focus on executive power and technology regulation.

Professor Rozenshtein files this brief because the case raises questions of exceptional importance concerning the scope of defense procurement authorities and the proper interpretation of statutes designed to protect national security systems from foreign adversary exploitation—questions on which his scholarship and prior government service uniquely position him to assist the Court. He has written and commented on the legal questions presented in this case since reporting of the government's planned "supply chain risk" designation first emerged. *See* Michael Endrias & Alan Z. Rozenshtein, *Pentagon's Anthropic Designation Won't Survive First Contact with Legal System,* Lawfare (Mar. 2, 2026), lawfaremedia.org/article/pentagon%27s-anthropic-designation-won%27t-survive-first-contact-with-legal-system; Alan Z. Rozenshtein & Benjamin Wittes, *The Situation: Stand with Anthropic*, Lawfare (Mar. 2, 2026), lawfaremedia.org/article/the-situation--stand-with-anthropic; Alan Z. Rozenshtein, *What the Defense Production Act Can and Can't Do to Anthropic*, Lawfare (Feb. 25, 2026), lawfaremedia.org/article/what-the-defense-production-act-can-and-can't-do-to-anthropic; Alan Z. Rozenshtein, *Congress—Not the Pentagon or Anthropic—Should Set Military AI Rules*, Lawfare (Feb. 20, 2026), lawfaremedia.org/article/congress-not-the-pentagon-or-anthropic-should-set-military-ai-rules.[1]

This brief addresses the proper interpretation of the statutory authorities the Department of Defense invokes to justify its designation of Anthropic as a "supply chain risk." Those authorities—

[1] No party or party's counsel authored this brief in whole or in part, and no party or party's counsel contributed money that was intended to fund the preparation or submission of this brief. No other person contributed money that was intended to fund the preparation or submission of this brief.

10 U.S.C. § 3252 and 41 U.S.C. § 4713—were enacted to protect sensitive government systems from covert hostile action through the information and communications technology supply chain. As their text makes clear, they target the risk that an adversary might "sabotage, maliciously introduce unwanted function, or otherwise subvert" the integrity of government systems. 10 U.S.C. § 3252(d)(4); *see* 41 U.S.C. § 4713(k)(6). Their structure and history confirm the same focus: foreign espionage and covert supply-chain compromise, not ordinary disputes with domestic vendors.

That threat model bears no resemblance to the circumstances of this case. Anthropic's dispute with the Department of Defense concerns disclosed contractual limitations on how its artificial intelligence (AI) model may be used—limitations that were known to the government from the outset of the parties' relationship and that the Department deliberately incorporated into its contracts with the company. Whatever the merits of the Department's subsequent policy disagreement with those restrictions, a negotiated contractual term cannot plausibly constitute "sabotage," the "malicious introduction of unwanted function," or any other form of covert supply-chain exploitation contemplated by the statutes Congress enacted. And even if it could, Secretary Hegseth's order—which purports to forbid defense contractors from maintaining even *commercial* relationships with Anthropic—far exceeds his limited statutory authority to restrict the Department's own *contracting* or *subcontracting* with designated entities. Congress knows how to write a broad commercial-activity restriction—as it did just months before enacting Section 4713, when it banned contractors from even *using* Huawei and ZTE equipment. *See* Pub. L. No. 115-232 § 889(a) (2018). Yet Congress used materially different language here.

Interpreting Sections 3252 and 4713 to reach this policy dispute would dramatically expand those provisions beyond their text and intended role. Authorities that Congress crafted to defend government systems against clandestine foreign espionage would become tools for regulating the commercial relationships between the government and domestic technology firms, permitting agencies to override long-established statutory and regulatory mechanisms for resolving disputes

with their contractors by jumping straight to complete supply-chain exclusion. The Court should not adopt that interpretation.

ARGUMENT

I. Sections 3252 and 4713 Were Designed to Address Foreign Espionage Through The Information and Telecommunications Technology Supply Chain.

The Department's designation of Anthropic cannot be reconciled with the history and structure of the two statutory authorities the Department invokes: 10 U.S.C. § 3252 and 41 U.S.C. § 4713. Section 3252 was enacted in 2011 to give the Department of Defense authority to address the risk that a foreign adversary might infiltrate or sabotage national security systems through the introduction of malicious code through the supply chain. The Federal Acquisition Supply Chain Security Act (FASCSA), which contains Section 4713, was enacted 7 years later to address concerns that foreign adversaries—and companies beholden to those foreign adversaries—could further target national security through infrastructure, such as power grids and financial systems, that were outside the scope of the Department of Defense's authority. Neither authority was intended to reach domestic companies embroiled in disputes over the terms of use of their technology.

Section 3252. Section 3252 is a defense-specific statute that applies to procurements for national security systems and related items. *See* 10 U.S.C. § 3252(d)(3), (5)-(6). The statute permits the Secretaries of Defense, Army, Navy, and Air Force to take certain "covered procurement actions" when found "necessary to protect national security by reducing supply chain risk." 10 U.S.C. §§ 3252(a)(1), (b)(2)(a), (d)(2). To take such an action, the relevant Secretary is required to first "mak[e] a determination in writing" that confirms such exclusion "is necessary to protect national security by reducing supply chain risk," and that "less intrusive measures are not reasonably available to reduce such supply chain risk." 10 U.S.C. § 3252(b)(2). The statute defines a supply chain risk as the "risk that an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a covered system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system." 10 U.S.C. § 3252(d)(4).

Section 3252 originated as a provision in the 2011 National Defense Authorization Act (NDAA). *See* Pub. L. No. 111-383, § 806 (2011). That authority, known originally as Section 815, was temporary. *See id.* But it was extended by another NDAA in 2013, *see* Pub. L. No. 112-239 § 806 (2013); made permanent and codified as 10 U.S.C. § 2339a in 2018, *see* Pub. L. No. 115-232 (2018); and renumbered as Section 3252 as part of a comprehensive reorganization of Title 10's acquisition provisions in 2021, *see* Pub. L. No. 116-283 (2021). Section 3252's operative provisions—including the definition of supply chain risk and the authority it grants—have remained substantively unchanged throughout.

Section 3252's predecessor provision—Section 815—was passed against the backdrop of what federal officials described as "the most significant breach of U.S. military computers ever." William J. Lynn III, *Defending a New Domain: The Pentagon's Cyberstrategy*, 89 Foreign Aff. 97, 97–98 (Sept./Oct. 2010). In 2008, malicious code created by a foreign intelligence agency was introduced to computers at the U.S. Central Command via a USB flash drive. *Id.* The Pentagon spent months eradicating the malware in an operation codenamed Buckshot Yankee—an effort so consequential it led to the creation of U.S. Cyber Command. *U.S. Cyber Command: Organizing for Cyberspace Operations: Hearing Before the H. Comm. on Armed Services*, 111th Cong. 9–10 (2010) (statement of Gen. Keith B. Alexander, Commander, U.S. Cyber Command).

The Senate Armed Services Committee's report on Section 815 makes clear that the statute was crafted in response to covert foreign threats to Department of Defense systems through the supply chain. The Committee Report states that the provision was intended to address threats identified by a "December 22, 2009 . . . report [by the Secretary of Defense] on trusted defense systems." S. Rep. 111-201, at 162 (2010). In that report, "the Secretary found that the globalization of the information technology industry has increased the vulnerability of the Department of Defense (DOD) to attack on its systems and networks"—in particular, that "systems and networks critical to DOD could be exploited through the introduction of counterfeit or malicious code and other defects introduced by suppliers of systems or components." *Id*. (emphasis added). Congress thus enacted

Section 815 because "the Secretary should have the authority needed to address this risk" of covert threats posed by the globalization of IT supply chains. *Id.*

Section 4713. Building on agency-specific authorities like Section 3252, Congress enacted FASCSA in 2018 to enable a broader set of agencies to coordinate their responses and defenses against supply chain infiltration and sabotage. Although "the United States security agencies ha[d] understood the threat to national security systems posed by ICT [information and communications technology] supply chains" for years, they also had to "grappl[e] with how to appropriately share classified information and address the risk for all government agencies." S. Rep. 115-408, at 4 (2018) ("FASCSA Committee Report"). FASCSA allows agencies to coordinate through "a whole-of government approach to supply chain risk management by creating a council and providing executive agencies with the necessary authorities to effectively share information and mitigate supply chain risks when procuring information and communications technology (ICT)." *Id.* at 1.

FASCSA adopted two mechanisms to address supply chain risks from hostile foreign actors. First, FASCSA created a new committee—the Federal Acquisition Security Council (FASC)—and directed it to develop "standards, guidelines, and practices" for federal agencies to use in addressing supply chain risks. 41 U.S.C. § 1326. It also authorized the FASC to make supply chain risk mitigation recommendations to the heads of specified executive agencies, who in turn were empowered to adopt the FASC's recommendations. 41 U.S.C. § 1323. Second, FASCSA authorized the Department of Homeland Security, the Department of Defense, and the Office of the Director of National Intelligence collectively to issue removal or exclusion orders that would result in "governmentwide exclusion" of a source from the supply chain. 41 U.S.C. § 1323.

In addition to establishing this system for coordinated, governmentwide responses, FASCSA also enacted Section 4713—the second provision the Department of Defense has invoked against Anthropic. Congress viewed Section 4713 and Section 3252 as closely related, recognizing that "existing authority"—namely, Section 3252's predecessor—already allowed "the Department of Defense [to] perform many of the activities described in" Section 4713. FASCSA Committee Report at 16. Yet despite the existence of Section 3252 and other agency-specific authorities, Congress

viewed Section 4713 as integral to a more "cohesive framework" for "swiftly address[ing] ICT supply chain issues." *Id.* at 7. Accordingly, Section 4713 is structured similarly to the Department of Defense's authority under Section 3252, but authorizes a broader set of agency heads to issue orders in response to supply chain risks in information-technology procurements. 41 U.S.C. § 4713.

II. Sections 3252 and 4713 Cannot Be Applied to Designate Anthropic a Supply Chain Risk.

Neither Section 3252 nor Section 4713 authorizes the Department's designation of Anthropic as a "supply chain risk." The statutes' text forecloses that designation; their structure confirms the limited scope; and their legislative history removes any doubt.

A. The Statutes' Definitions of "Supply Chain Risk" Do Not Authorize the Secretary to Designate Anthropic a Supply Chain Risk.

Statutory text forecloses the Department's designations in three separate respects. *First*, the definitions of "supply chain risk" in Sections 3252 and 4713—definitions that mark the scope of each provision—have no plausible application to Anthropic. Both statutes define supply chain risk by reference to clandestine, hostile conduct: covert actions seeking to sabotage, subvert, or surveil those systems without the government's knowledge. The statutory language describes a threat that operates in secret and against the interests of the United States—not a vendor that negotiates in good faith over the permissible uses of its own technology.

Section 3252 defines "supply chain risk" as the risk that "an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a covered system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system." 10 U.S.C. § 3252(d)(4). Section 3252 thus plainly contemplates unanticipated actions by malicious foreign actors ("adversar[ies]") to infiltrate Department of Defense systems, either to "disrupt" their functions or to "surveil" their conduct. Section 4713 uses a nearly identical formulation, defining "supply chain risk" to mean "the risk that any person may sabotage, maliciously introduce unwanted function, extract data, or otherwise manipulate the design, integrity, manufacturing, production,

distribution, installation, operation, maintenance, disposition, or retirement of covered articles so as to surveil, deny, disrupt, or otherwise manipulate the function, use, or operation of the covered articles or information stored or transmitted on the covered articles." 41 U.S.C. § 4713(k)(6).

The dispute over the terms of the Department's use of Anthropic's AI model are plainly not "sabotage," "malicious introduction of unwanted function," or "subversion" of sensitive national security systems. Anthropic refused to authorize two specific applications of its technology: mass domestic surveillance of Americans and fully autonomous weapons systems intended to kill humans without human oversight. Those restrictions were disclosed from the outset of the parties' contractual relationship—and indeed were part of the contract the Department of Defense signed with Anthropic in the summer of 2025. *See* Anthropic's Notice of Motion and Motion for a Temporary Restraining Order, Preliminary Injunction, or Section 705 Stay ("Mot."), ECF No. 6, at 5–6. A known, disclosed, commercially negotiated limitation on permissible use is a far cry from the covert, hostile acts that the statute describes.

Second, Anthropic is not the type of entity that can be designated a supply chain risk in the first place. Section 3252 addresses threats posed by "adversar[ies]." Though that term is undefined, Department of Defense instructions implementing Section 3252 that were published shortly after enactment underscored that the focus of the statute is on "foreign intelligence, terrorists, or other hostile elements." Dep't of Def., Instruction 5200.44, Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN) § 1.a (Nov. 5, 2012), perma.cc/TW3D-735M (targeting "sabotage or subversion of a system's mission critical functions or critical components" by these entities). This is consistent with the text of the rest of the statute, which assumes "adversar[ies]" are entities that "sabotage," "subvert," and "maliciously introduce unwanted function" into Department of Defense systems. 10 U.S.C. § 3252(d)(4). A U.S.-based software vendor in a policy dispute plainly does not fit the bill.

Similarly, Section 4713 addresses supply chain risks arising from "any person" who may "sabotage, maliciously introduce unwanted function, extract data, or otherwise manipulate" Department of Defense systems. 41 U.S.C. § 4713(k)(6). Although Section 4713 refers to "any

person," its parallel focus on sabotage, malicious introduction, and covert manipulation confirms that it addresses the same kind of hostile supply-chain threats that Section 3252 addresses in the defense context. FASCSA simply extends that framework across the broader procurement system.

Third, even if these statutes could reach Anthropic, the Secretary's orders here are vastly overbroad and *ultra vires*. Section 3252 permits only three "covered procurement actions": (1) excluding a source based on qualification standards, (2) excluding a source based on evaluation factors, and (3) directing a contractor to exclude a source from subcontracting on a covered system. 10 U.S.C. § 3252(d)(2). Section 4713 authorizes the same three actions, along with determinations that a specified entity is not a "responsible source"—determinations that, like the other three, are limited to that entity's ability to *contract* with the Department. 41 U.S.C. § 4713(k)(3); *see id.* § 113.

To be sure, the statutes' references to "subcontracting" give them some downstream reach—the Department can direct a prime contractor not to subcontract to Anthropic on a covered system. But the Secretary's "final" directive posted on social media goes far beyond subcontracting consent. Mot. at 16–17, 19. It purports to bar all Defense Department contractors from "partner[ing]" or "conduct[ing] any commercial activity" with Anthropic, regardless of whether that business is within the scope of a Department contract. *Id.* at 16. Taken at face value, defense contractors could not use Anthropic's products for their own non-government purposes—or even *sell* to Anthropic. When the government has previously sought comparable restrictions, it has required an act of Congress. Section 889 of the 2019 NDAA—enacted just months before FASCSA—expressly bars federal agencies from contracting with any entity that "uses" covered telecommunications equipment—including equipment from Huawei and ZTE—as a substantial component "of any system." *See* Pub. L. No. 115-232 § 889(a) (2018). The Secretary should not be permitted to impose the same secondary-boycott effect—and then some—through a narrow procurement statute.

B. Additional Textual and Structural Features of the Statutes Confirm They Cannot Be Used to Designate Anthropic as a Supply Chain Risk.

Beyond their definitions of supply chain risk, the statutes contain additional features that confirm they cannot plausibly be applied to Anthropic. Most critically, Section 3252 and 4713 both require that an agency head must—before cutting the vendor out of the procurement supply chain—make a written determination that "less intrusive measures are not reasonably available to reduce . . . supply chain risk." 10 U.S.C. § 3252(b)(2)(B); 41 U.S.C. § 4713(b)(3)(B). But in disputes like this one—where the alleged "risk" arises from one contracting party's refusal to cede to the demands of the other contracting party to remove previously settled mutually negotiated usage restrictions—ordinary procurement tools will always be available to address the government's concerns. The agency could negotiate revised terms, it could terminate the contract for its own convenience, or it could re-solicit new solutions based on any changed needs of the government. Any of these steps would resolve the government's stated concern without the extraordinary measure of cutting the supplier (its affiliates and all their products and services) out of the procurement system altogether. Only with *covert* risks will the least intrusive measure be wholesale exclusion from government contracts.

Indeed, a contrary reading would supplant much of the federal procurement system—jeopardizing untold numbers of government contracts without the "clear congressional authorization" that such a major transformation would require. *West Virginia v. EPA*, 597 U.S. 697, 721 (2022); *see Learning Res., Inc. v. Trump*, No. 24-1287, 2026 WL 477534, at *7 (U.S. Feb. 20, 2026) (plurality opinion) ("We have long expressed reluctance to read into ambiguous statutory text extraordinary delegations of Congress's powers." (quotation omitted)). The complex, sprawling set of procurement statutes and rules that regulate government contracting—including Title 41 and the Federal Acquisition Regulation—include myriad provisions allowing for the orderly resolution of contract disputes, ranging from administrative contract claims, to termination, to suspension and

debarment.[2] If any company which failed to revisit or renegotiate previously agreed upon terms could be deemed a supply chain risk, an agency could readily short-circuit this specialized framework by jumping directly to outright exclusion of the supplier from procurement system—with little to no process. From the perspective of current or prospective contractors, the ever-present threat of complete exclusion (and corresponding reputational harm) would make the risks and costs of government contracting skyrocket, discouraging participation in the federal marketplace. Reading Congress's narrow anti-sabotage protections to permit the government to exclude domestic vendors, sever commercial relationships across the defense industrial base, and override negotiated contract terms—bypassing the entire dispute-resolution framework Congress built for precisely these situations—would be to "hide elephants in mouseholes." *Whitman v. Am. Trucking Associations*, 531 U.S. 457, 468 (2001).

Were more needed, the defendants' interpretation of Section 3252 threatens serious constitutional problems that could readily be avoided through adherence to its plain text. Section 3252 largely deprives designated entities of any notice, an opportunity to respond, or a right to judicial review of decisions to withhold the reasons for the designation. *See* 10 U.S.C. § 3252. Instead, the Secretary need only make a written determination—which he can withhold from public and even the contractor's view—that designating the entity is "necessary to protect national security by reducing supply chain risk" and that "less intrusive measures are not reasonably available to

[2] *See, e.g.*, 41 U.S.C. §§ 7101–7109 (Contract Disputes Act (CDA)), establishing comprehensive framework for resolving disputes arising under government contracts, including claims for equitable adjustment and appeals to the Agency Board of Contract Appeals or the Court of Federal Claims); 48 C.F.R. § 52.233-1 (mandatory "disputes" clause, requiring contractors to "proceed diligently with performance of this contract, pending final resolution of any request for relief, claim, appeal, or action arising under or relating to the contract"); 48 C.F.R. § 52.212-4(d) (commercial products and services clause, directing that failure to reach agreement on "any request for equitable adjustment, claim, appeal or action arising under or relating to this contract shall be a dispute to be resolved" through the CDA mechanism); 48 C.F.R. § 52.249-2 (termination for convenience, providing the government's established mechanism to exit a contract when a contractor's terms are no longer acceptable); 48 C.F.R. Part 49 (termination for convenience or default, including equitable adjustment of price and settlement of costs); 48 C.F.R. Subpart 9.4 (suspension and debarment procedures, providing the proper mechanism for excluding contractors on responsibility grounds, with notice and an opportunity to respond); 48 C.F.R. § 9.402(b) (requiring that exclusion from procurement "be imposed only in the public interest for the Government's protection and not for purposes of punishment").

reduce such supply chain risk." *Id.* § 3252(b); *see* § 3252(a)(2), (3) (allowing the Secretary to "limit . . . the disclosure of information relating to the basis for carrying out a covered procurement action"). Congress designed this stripped-down process for a reason: It assumed the targets would be foreign "adversar[ies]" and other entities with attenuated (if any) claims to procedural protections under the Due Process Clause. Domestic companies, by contrast, have a liberty and property interest in not being deprived of existing government contracts without notice or an opportunity to be heard. *See Old Dominion Dairy Products, Inc. v. Secretary of Defense*, 631 F.2d 953, 969 (1980). Interpreting Section 3252 to reach companies like Anthropic, which enjoy the full panoply of due process protections, would therefore put the statute in conflict with the Due Process Clause. The canon of constitutional avoidance thus demands reading Section 3252 more narrowly.

C. The Legislative History of Section 3252 and 4713 Confirms that the Department Cannot Use the Statutes to Designate Anthropic as a Supply Chain Risk.

If there were any doubt that the text of Sections 3252 and 4713 cannot be used to designate Anthropic a supply-chain risk, their entwined legislative histories confirm that both statutes were intended to address foreign intelligence threats to the integrity of defense and other government systems.

The Committee Report on Section 815—the provision that became Section 3252—makes clear that the statute is directed at covert foreign threats. The Committee explained that the provision was intended to give the Secretary of Defense the "authority needed to address th[e] risk[s]" posed by "the globalization of the information technology industry." S. Rep. 111-201, at 162 (2010). In particular, Section 3252 was crafted to address the "increased . . . vulnerability of the Department of Defense (DOD) to attacks on its systems and networks" and the "exploit[ation]" of "systems and networks critical to DOD . . . through the introduction of counterfeit or malicious code and other defects introduced by suppliers of systems or components." *Id.*

The rationale behind Section 815, then, centered on the risk that malicious code might infiltrate defense systems through the supply chain. Nothing in the Committee's stated justification

of Section 3252 contemplates—or could reasonably be read to encompass—a dispute with an American software company over use restrictions of its own product. The historical context in which Section 815 was passed underscores this. As explained, Section 815 was created shortly after malicious code created by a foreign intelligence agency infected computers at the U.S. Central Command.

As with Section 3252, Congress included Section 4713 as part of FASCSA to address concerns about the infiltration and sabotage of U.S. government systems by hostile foreign actors. The Senate Homeland Security and Government Affairs Committee Report on FASCSA specifically recognized the interrelation between the two authorities: Section 3252's predecessor already allowed "the Department of Defense [to] perform many of the activities described in" Section 4713. FASCSA Committee Report at 16. Yet Congress believed it necessary to enact a similarly structured provision—Section 4713—as part of its "cohesive framework" for "swiftly address[ing] ICT supply chain issues." *Id.* at 7. There is no indication that Congress viewed Section 4713's definition of supply chain risk as sweeping more broadly than Section 3252 or that Congress intended to confer broader authorities than it had previously given to the Department of Defense. To the contrary, the Committee explained that Section 4713, like Section 3252, sought to prevent covert exploitation. It explained that "[h]ostile nation states and other bad actors are attempting to gain unprecedented access to sensitive and classified information via the Federal ICT supply chains." *Id.* at 2. The Committee further observed that "[m]any of the technologies the Federal Government relies on for vital, daily functions either could be or already have been targeted by bad actors or hostile nation states." *Id.*

The Committee highlighted that its concern focused on companies beholden to hostile foreign regimes, not domestic companies in contractual disputes. The Committee warned that "[t]he U.S. government must pay particular attention to products produced by companies with ties to regimes that present the highest and most advanced espionage threats to the U.S., such as China." *Id.* at 3. It specifically flagged that "[m]alicious Chinese hardware or software implants would . . . be a potent espionage tool." *Id.* at 2 n.4 (internal citations omitted). And it echoed FBI

Director Christopher Wray's "deep[] concern[]" about "the risks of allowing any company or entity that is beholden to foreign governments that don't share our values to gain positions of power inside our telecommunications networks," because such access "provides the capacity to maliciously modify or steal information, and it provides the capacity to conduct undetected espionage." *Id.* at 3.

The Committee Report identified two recent supply chain risk incidents as catalysts for the enactment of FASCSA—further confirming that the statute was directed at covert infiltration by companies beholden to hostile foreign governments. First, in 2017, the Department of Homeland Security (DHS) determined that a Russia-based anti-virus software from AO Kaspersky Lab, which was used in some federal civilian executive agencies, could be sharing data obtained from the agencies with the Russian government. *Id.* at 4–6. DHS issued a Binding Operational Directive ordering federal civilian executive agencies to identify and remove Kaspersky products from their information systems, but the order was then challenged in court and was on appeal at the time the FASCSA Committee Report was issued. *Id.* at 5–6. Second, in 2018, Congress banned the use of telecommunications equipment manufactured by two Chinese-based companies, Huawei Technologies Company and ZTE Corporation. *Id.* at 6. The ban came after a hearing in which the directors of several intelligence agencies "were each asked if they would use products or services from Huawei or ZTE; all answered in the negative." *Id.*

The legislative histories of Sections 3252 and 4713 thus confirm that the statutes were enacted to protect government systems from covert hostile action by foreign actors. Every threat the Committees identified was foreign in origin, clandestine in nature, and aimed at compromising the integrity of government systems without the government's knowledge.

Anthropic is none of these things. It is an American company that forthrightly disclosed its usage restrictions, negotiated them in good faith with the Department of Defense, and incorporated them into the very contract the Department executed in the summer of 2025. The dispute that followed can be resolved through other means. Congress enacted Sections 3252 and 4713 to confront a fundamentally different problem, and stretching those authorities to cover a dispute with a domestic software provider would exceed their text and purpose. Authorities crafted to prevent

clandestine exploitation by actors like Kaspersky, Huawei, and ZTE cannot plausibly be repurposed to punish an American company for maintaining publicly disclosed, and previously agreed-upon restrictions on the use of its own technology.

CONCLUSION

The Court should enjoin or stay the defendants' actions.

Dated: March 11, 2026

By: */s/ Allyson Myers*
Elisabeth S. Theodore (*pro hac vice* to be filed)
Benjamin C. Mizer (*pro hac vice* to be filed)
Eun Young Choi (*pro hac vice* to be filed)
Samuel F. Callahan (*pro hac vice* to be filed)
Aaron X. Sobel (*pro hac vice* to be filed)
Allyson Myers (SBN 342038)

ARNOLD & PORTER
KAYE SCHOLER LLP

Attorneys for Amicus Curiae Alan Z. Rozenshtein