

Todd C. Toral (SBN CA 197706)
JENNER & BLOCK LLP
2029 Century Park East, Suite 1450
Los Angeles, CA 90067-2901
Telephone: +1 213 239 6900
TToral@jenner.com

Matthew Klapper (SBN DC 90035346)*
JENNER & BLOCK LLP
1099 New York Avenue, NW Suite 900
Washington, DC 20001-4412
Telephone: +1 202 639 6000
MKlapper@jenner.com

Counsel for Amici Curiae Leon Panetta and the Institute for Security and Technology

**Pro hac vice forthcoming.*

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA**

ANTHROPIC PBC,

Plaintiff,

v.

UNITED STATES DEPARTMENT OF WAR, et
al.,

Defendants.

Case No. 3:26-cv-01996

**BRIEF OF AMICI CURIAE FORMER
SECRETARY OF DEFENSE LEON
PANETTA AND THE INSTITUTE FOR
SECURITY AND TECHNOLOGY IN
SUPPORT OF PLAINTIFF'S MOTION FOR
SUMMARY JUDGMENT**

Judge: Hon. Rita F. Lin
Ctmm: 15, 18th Floor
Date: July 30, 2026
Time: 10:00 A.M.

TABLE OF CONTENTS

TABLE OF AUTHORITIES i

IDENTITIES AND INTERESTS OF *AMICI CURIAE* 1

INTRODUCTION AND SUMMARY OF ARGUMENT 2

ARGUMENT..... 3

I. THE DEPARTMENT’S SUPPLY CHAIN RISK DESIGNATION WAS UNJUSTIFIED
AND UNDERMINES ITS CREDIBILITY..... 3

 A. THE DEPARTMENT’S DESIGNATION OF ANTHROPIC WAS
 PRETEXTUAL, AND FAR EXCEEDED WHAT WAS NECESSARY TO
 ADDRESS THE SUPPOSED THREAT..... 4

 B. PRETEXTUAL USE OF THIS SIGNIFICANT AUTHORITY UNDERMINES
 THE CREDIBILITY OF THE DEPARTMENT WITH INDUSTRY AND THE
 PUBLIC..... 8

II. IMPROPER DESIGNATION OF ANTHROPIC AS A SUPPLY CHAIN RISK
THREATENS THE U.S.’S MILITARY AND ECONOMIC ADVANTAGE AT A
PIVOTAL MOMENT IN U.S.–CHINA TECHNOLOGICAL COMPETITION..... 12

CONCLUSION..... 14

TABLE OF AUTHORITIES**Page(s)****Cases**

<i>Georgia v. President of the U.S.</i> , 46 F.4th 1283 (11th Cir. 2022).....	7
<i>Greer v. Spock</i> , 424 U.S. 828 (1976)	8
<i>Perkins v. Lukens Steel Co.</i> , 310 U.S. 113 (1940)	7

Statutes

10 U.S.C § 3252.....	2, 3
10 U.S.C. § 3252(b)(2)(B).....	6, 8
10 U.S.C. § 3252(d)(4).....	3

Legislative Materials

S. Rep. No. 111-201 (2010).....	5
---------------------------------	---

Other Authorities

48 C.F.R. § 9.103	6
48 C.F.R. § 9.104-1(d).....	6
48 C.F.R. § 9.104-4.....	6
48 C.F.R. § 9.402(b).....	6
48 C.F.R. § 42.1303	6
48 C.F.R. § 49.101(b).....	6
48 C.F.R. § 49.402-3	6
48 C.F.R. § 52.212-4(m).....	6
48 C.F.R. § 52.242-15	6
48 C.F.R. § 52.243-4	6
48 C.F.R. § 52.249-1-52.249-6	6

1	2025 Reagan National Defense Survey, Ronald Reagan Inst. (Nov. 2025),	
2	https://www.reaganfoundation.org/reagan-institute/centers/peace-through-strength/survey/2025-reagan-national-defense-survey	9
3	<i>Assessing Claude Mythos Preview's Cybersecurity Capabilities</i> , Anthropic Red Team	
4	(Apr. 7, 2026), https://red.anthropic.com/2026/mythos-preview/ ;.....	11
5	Anisha Sircar, <i>Anthropic Disabled Fable 5 and Mythos 5 After a U.S. Export-Control order. Here's What Happened</i> , Forbes (June 16, 2026)	
6	https://www.forbes.com/sites/anishasircar/2026/06/16/anthropic-disabled-fable-5-and-mythos-5-after-a-us-export-control-order-heres-what-happened/ ;.....	5
7		
8	Cristina Criddle & Demetri Sevastopulo, <i>US National Security Agency Using Anthropic's Mythos for Cyber Attacks</i> , Fin. Times (June 4, 2026),	
9	https://www.ft.com/content/d02d91b3-2636-454e-9442-dc7e69f51815?syn-25a6b1a6=1	4
10		
11	David Montgomery, <i>Many Americans Think AI Companies Should Be Able to Limit How the U.S. Military Uses Their Tools</i> , YouGov (Mar. 10,	
12	2026), https://yougov.com/en-us/articles/54285-many-americans-think-ai-companies-should-be-able-to-limit-how-us-military-uses-tools-march-6-9-2026-economist-yougov-poll	9
13		
14	Dean Ball, <i>Clawed</i> , Hyperdimensional (Mar. 2, 2026),	
15	https://www.hyperdimensional.co/p/clawed	14
16	Dep't of Def., Instr. 5200.44, Protection of Mission Critical Functions to Achieve Trusted Sys. and Networks (TSN) (Nov. 5, 2012).....	6
17		
18	Donald J. Trump (@realDonaldTrump), Truth Social (Feb. 27, 2026),	
19	https://truthsocial.com/@realDonaldTrump/posts/116144552969293195	6
20		
21	Fatima Faisal Khan, <i>The Missing Middle</i> , Inst. for Sec. + Tech. (Oct. 2025).....	13
22		
23	Jake Bleiberg & Margi Murphy, <i>White House Works to Give US Agencies Anthropic Mythos Access</i> , Bloomberg (Apr. 16, 2026).....	8
24		
25	Karen Freifeld, <i>Big Tech Group Tells Pentagon's Hegseth They Are 'Concerned' About Anthropic Supply-Chain Risk Designation</i> , Reuters (Mar. 4, 2026).....	10
26		
27	Kate Conger & David E. Sanger, <i>Pentagon Cancels a Disputed \$10 Billion Technology Contract</i> , N.Y. Times (July 6, 2021)	7
28		
	Kyle Chan et al., <i>Full Stack: China's Evolving Industrial Policy for AI</i> , RAND (June 26, 2025).....	12
	Leon Panetta, Panetta Inst., https://www.panettainstitute.org/about-us/institute-people/leon-panetta/	1

1	Luke Emberson, <i>Chinese AI Models Have Lagged the US Frontier by 7 Months On</i>	
2	<i>Average Since 2023</i> , Epoch AI (Jan. 2, 2026).....	12
3	Mike Stone et al., <i>Hegseth Wants Pentagon to Dump Anthropic's Claude, But Military</i>	
4	<i>Users Say It's Not So Easy</i> , Reuters (Mar. 19, 2026).....	10
5	Mike Stone, <i>Pentagon Deploys Anthropic's Mythos to Patch Cyber Gaps While</i>	
6	<i>Planning to Ditch Firm</i> , Reuters (May 12, 2026).....	4
7	<i>Nation State Threats</i> , CISA, https://www.cisa.gov/topics/cyber-threats-and-	
8	advisories/nation-state-cyber-actors	9, 10
9	Nick Wakeman, <i>Pentagon Hits Accenture, Booz Allen and Deloitte with Contract</i>	
10	<i>Cancellations</i> , Wash. Tech. (Apr. 11, 2025), https://www.washington-	
11	tech.com/2025/04/hits-accenture-	
12	booz-allen-and-deloitte-contract-cancellations/404500/	7
13	<i>Our Evaluation of Claude Mythos Preview's Cyber Capabilities</i> , UK AI Sec. Inst.:	
14	Blog (Apr. 13, 2026), https://www.aisi.gov.uk/blog/our-evaluation-of-claude-	
15	mythos-previews-cyber-capabilities	11, 12
16	Pablo Chavez, <i>The Sovereignty Gap in U.S. AI Statecraft</i> , Lawfare (Feb. 16, 2026),	
17	https://www.lawfaremedia.org/article/the-sovereignty-gap-in-u.s.-ai-statecraft	13-14
18	Pete Hegseth (@SecWar), X (Feb. 27, 2026), https://x.com/SecWar/status/2027507717	
19	469049070	6
20	<i>Project Glasswing: An Initial Update</i> , Anthropic (May 22, 2026),	
21	https://www.anthropic.com/research/glasswing-initial-update	11
22	Robert Brodsky, <i>GAO: Major Defense Contracts Cheaper to Cancel Than Continue</i> ,	
23	Gov't Exec. (Mar. 19, 2008), https://www.govexec.com/defense/2008/03/gao-	
24	major-defense-contracts-cheaper-to-cancel-than-continue/26527	7
25	<i>Statement on the US Government Directive to Suspend Access to Fable 5 and Mythos</i> ,	
26	Anthropic (Jun. 12, 2026)	5
27	Scott Singer & Matt Sheehan, <i>China's AI Policy at the Crossroads: Balancing</i>	
28	<i>Development and Control in the DeepSeek Era</i> , Carnegie Endowment for Int'l	
	Peace (July 17, 2025).....	13
	<i>To Support and Defend: Principles of Civilian Control and Best Practices of Civil-</i>	
	<i>Military Relations</i> , War on the Rocks (Sept. 6, 2022).....	8

IDENTITIES AND INTERESTS OF *AMICI CURIAE*¹

Amici have a strong interest in this case, which lies at the intersection of significant civilian military authorities and technological advancements, national security, and global stability. They submit this brief to provide the Court with the views and expertise of a former leader of the Department of War (“Department”), and researchers who work to unite policymakers, technology experts, and industry leaders behind the development of trustworthy, non-exploitative, and non-negligent technologies.

Amicus former Secretary of Defense Leon Panetta² has directed the Nation’s military through numerous armed conflicts and has managed countless relationships between the government and the private sector that have materially enhanced American military capabilities. Secretary Panetta helped shepherd emerging technologies into appropriate use and deployment by the Armed Forces and appreciates how essential it is to maintain the trust and cooperation of private sector partners on whom the Department depends. He understands, through direct experience, the gravity and responsibility of deploying the Department’s most severe sanctions, including those designed to address threats to national security, and he is uniquely positioned to speak to the need to do so in a manner that protects the credibility of the Department in the eyes of industry and the American public.

Amicus the Institute for Security and Technology (“IST”) is a critical action think tank dedicated to the development of trustworthy technologies that advance national security and global stability, and the study of policy that fosters such technological development and builds trust between industry, civic leaders, technology experts, and government. IST has been especially focused on the impact of the American developers of artificial intelligence (“AI”) on global stability, and the interaction between those developers and government actors. Through its research, IST has developed a special expertise in AI security and the need to maintain American leadership in AI over China.

¹ No counsel for any party authored this brief in whole or in part. No person other than *amici* or their counsel contributed money intended to fund this brief’s preparation or submission.

² A brief biography of Secretary Panetta can be found at *Leon Panetta*, Panetta Inst., <https://www.panettainstitute.org/about-us/institute-people/leon-panetta/>.

1 *Amici* understand that the government protects national security while private industry drives
 2 technological innovation—innovation that, in turn, drives American economic and national security.
 3 They are profoundly committed to the appropriate deployment of the authorities of the Department in a
 4 manner that serves U.S. national security, as well as the need to ensure that advancements in
 5 technology—particularly in AI—also advance national security and global stability. *Amici* submit this
 6 brief to provide the Court with the perspective of a Department leader charged with safeguarding both
 7 national security and the institutional integrity and long-term credibility of the United States military,
 8 and of a group dedicated to seizing the opportunities created by and mitigating the potential harms of
 9 technology, and to understanding its impact on national security, global stability, and trust between
 10 industry, the government, and the public.

11 **INTRODUCTION AND SUMMARY OF ARGUMENT**

12 The Department’s decision to designate American artificial intelligence company Anthropic
 13 PBC a supply chain risk under 10 U.S.C § 3252 is a clear misuse of an authority designed to protect
 14 government systems from genuine threats to national security. It is a reactive gesture that threatens to
 15 upend the stability of the government’s relationship with its private sector partners—a stability on which
 16 American military and economic power depend. The consequences for the strength and credibility of
 17 the government are far-reaching, as the designation risks driving away the companies who provide
 18 technological capabilities critical to the functioning of a modern military and, through its punitive reach,
 19 undermining the American advantage in the race to develop the world’s best AI models.

20 Section 3252 is a substantial authority that should be used sparingly, and only to protect the
 21 country against real and serious risks to the integrity of government systems. It has never been used
 22 against an American company—and certainly never so publicly, and with such an expansive and
 23 detrimental impact on a vital national industry and on the American economy writ large. The
 24 government has never designated a company a supply chain risk—such that working with it would
 25 purportedly render an agency vulnerable to penetration by foreign and hostile entities—and nevertheless
 26 continued to explore working with and potentially even using its top-of-the-line technology. But here,
 27 the government, including the Department, continues to work with Anthropic to expand its use of
 28

1 Anthropic’s most important new model, Claude Mythos Preview (“Mythos”). The government seeks
 2 to benefit from Anthropic’s active collaboration by using Mythos, while simultaneously trying to
 3 leverage Anthropic into betraying its commercial interests and values through the section 3252
 4 designation. But section 3252 cannot bear the weight of that dissonance.

5 The designation will let China pull ahead in the AI race and make the military seem less
 6 trustworthy to its contracting partners—both of which will make the country less safe. Because that is
 7 not what Congress intended, and not how former Secretaries have conceived of the Department’s
 8 exceptional statutory authorities, the Court should grant Anthropic’s Petition for Review and enjoin the
 9 government’s section 3252 designation.

10 **ARGUMENT**

11 When the Department designated Anthropic a supply chain risk, its justification was pretextual.
 12 There is and was no evidence that the company poses any legitimate national security risk to government
 13 systems, and the government’s own statements suggest that the decision was motivated by a desire to
 14 punish the company for staking out a contractual position at odds with the Department’s own
 15 preferences. The government’s true assessment of Anthropic’s technology is laid bare by the
 16 government and the Department’s own ongoing use of Anthropic’s latest and most cutting-edge model,
 17 Mythos. Far from protecting U.S. national security, this pretextual designation threatens it in at least
 18 three ways: first, by eroding the credibility of the Department when trust in the institution could not be
 19 more critical; second, by denying the Department access to cutting-edge technology and thereby
 20 rendering it less effective in its mission; and third, by undercutting the country’s AI ecosystem and
 21 ceding technological leadership to China at a defining moment in geopolitical competition.

22 **I. THE DEPARTMENT’S SUPPLY CHAIN RISK DESIGNATION WAS** 23 **UNJUSTIFIED AND UNDERMINES ITS CREDIBILITY.**

24 10 U.S.C. § 3252 grants the Secretary of War the power to take certain procurement actions to
 25 designate a source a “supply chain risk” if it may “sabotage, maliciously introduce unwanted function,
 26 or otherwise subvert” a national security system. 10 U.S.C. § 3252(d)(4). Anthropic posed no such
 27 risk, yet the Department invoked this harsh sanction to cripple the company, seemingly out of
 28 ideological animus. Such a pretextual designation, particularly where the government’s continuing use

of Mythos is in tension with its stated views, has far-reaching effects for the Department's integrity, undermining public trust and making it harder for the nation's Armed Forces to do their job.

A. THE DEPARTMENT'S DESIGNATION OF ANTHROPIC WAS PRETEXTUAL, AND FAR EXCEEDED WHAT WAS NECESSARY TO ADDRESS THE SUPPOSED THREAT.

The Department's decision to target Anthropic was not motivated by concern about a legitimate supply chain risk. Until negotiations broke down between the Department and Anthropic, the Department appeared to be highly satisfied with both the company and its AI model, Claude. The government consistently granted Anthropic top-level security clearances and authorizations to support sensitive national security projects, as this Court has already recognized. *See* Order Granting Motion for Preliminary Injunction, ECF No. 134 at 5 (concluding that "The un rebutted record shows that, until this dispute, Anthropic 'only ever received positive feedback about Claude's performance from [its] governmental customers.'") (internal cited authorities omitted) (alteration in original). Even in the wake of the supply chain risk designation, public reporting suggests the government continues to expand, rather than wind down, its use of Anthropic's AI models. *See, e.g.,* Mike Stone et al., *Hegseth Wants Pentagon to Dump Anthropic's Claude, But Military Users Say It's Not So Easy*, Reuters (Mar. 19, 2026), <https://www.reuters.com/business/hegseth-wants-pentagon-dump-anthropics-claude-military-users-say-its-not-so-easy-2026-03-19/>. The Pentagon is apparently deploying a powerful new version of Claude, called Mythos, to find and patch cybersecurity vulnerabilities across the federal government. *See* Mike Stone, *Pentagon Deploys Anthropic's Mythos to Patch Cyber Gaps While Planning to Ditch Firm*, Reuters (May 12, 2026), <https://www.reuters.com/technology/pentagon-deploys-anthropics-mythos-patch-cyber-gaps-while-planning-ditch-firm-2026-05-12/>. Similarly, the NSA is apparently embedding Anthropic's engineers in the agency to assist in guiding its use of Mythos. *See* Cristina Criddle & Demetri Sevastopulo, *US National Security Agency Using Anthropic's Mythos for Cyber Attacks*, Fin. Times (June 4, 2026), <https://www.ft.com/content/d02d91b3-2636-454e-9442-dc7e69f51815?syn-25a6b1a6=1>. This is not the behavior expected of a government facing a national

1 security threat so grave it felt compelled to ban all departments and agencies from working with the
2 company.³

3 The novel designation also contravenes the statute. In a report discussing the threat of supply
4 chain risks to the Department of Defense as part of the National Defense Authorization Act for Fiscal
5 Year 2011, which laid the groundwork for the provision now codified at 10 U.S.C. § 3252, Congress
6 noted that “the globalization of the information technology industry has increased the vulnerability of
7 the Department of Defense (DOD) to attacks on its systems and networks.” S. Rep. No. 111-201, at
8 162 (2010). Congress was particularly worried about the “increasing risk that systems and networks
9 critical to DOD could be exploited through the introduction of counterfeit or malicious code and other
10 defects introduced by suppliers of systems or components,” and concluded that the Secretary of Defense
11 “should have the authority needed to address this risk.” *Id.* Indeed, the Department’s own instructions
12 acknowledge that the focus of the provision is “sabotage” or “subversion” by “foreign intelligence,
13 terrorists, or other hostile elements.” Dep’t of Def., Instr. 5200.44, Protection of Mission Critical
14 Functions to Achieve Trusted Sys. and Networks (TSN), § 1(a) (Nov. 5, 2012). Here, there is no
15 indication of *any* risk that Anthropic has enabled or could enable “foreign intelligence, terrorists, or
16 other hostile elements” to gain access to and “sabotage” or “subver[t]” Department systems and
17 networks, through “malicious code” or otherwise. *Id.* The government has neither asserted that
18 Anthropic is controlled by a foreign adversary or hostile element, nor has it publicly disclosed any
19 evidence that the company’s products are otherwise compromised by foreign control or espionage
20 activities. Further, there is no indication that Anthropic’s products – including its AI models – are

21
22
23 ³ Indeed, Anthropic’s new models are apparently so powerful that the Department of Commerce very
24 recently ordered that Anthropic suspend access to Mythos and another of its AI models still in
25 development, Fable 5, by any foreign national. *See Statement on the US Government Directive to*
26 *Suspend Access to Fable 5 and Mythos 5*, Anthropic (June 12, 2026),
27 <https://www.anthropic.com/news/fable-mythos-access>. According to the White House’s AI advisor,
28 their concerns about Mythos had nothing to do with the Department of War’s supply chain risk
designation. *See Anisha Sircar, Anthropic Disabled Fable 5 and Mythos 5 After a U.S. Export-Control*
Order. Here’s What Happened, Forbes (June 16, 2026),
<https://www.forbes.com/sites/anishasircar/2026/06/16/anthropic-disabled-fable-5-and-mythos-5-after-a-us-export-control-order-heres-what-happened/>.

1 somehow uniquely vulnerable to espionage activities. If the Pentagon truly believed they were, it would
 2 not be deploying one of the company’s most advanced AI models to patch its own cyber vulnerabilities.

3 The unprecedented public statements accompanying the designation reveal its true motivation:
 4 animus toward Anthropic, and a desire to retaliate against the company for disagreeing with the
 5 government about the operational use of its technology. *See, e.g.,* Donald J. Trump
 6 (@realDonaldTrump), Truth Social (Feb. 27, 2026), [https://truthsocial.com/@realDonaldTrump/](https://truthsocial.com/@realDonaldTrump/posts/116144552969293195)
 7 [posts/116144552969293195](https://truthsocial.com/@realDonaldTrump/posts/116144552969293195) (excoriating Anthropic as a “RADICAL LEFT, WOKE COMPANY”
 8 filled with “Leftwing nut jobs”); Pete Hegseth (@SecWar), X (Feb. 27, 2026),
 9 <https://x.com/SecWar/status/2027507717469049070> (accusing Anthropic of “attempt[ing] to strong-
 10 arm the United States military into submission—a cowardly act of virtue-signaling that places Silicon
 11 Valley ideology above American lives”). For this alleged “betrayal,” *see* Pete Hegseth (@SecWar), X
 12 Post, the Department escalated a straightforward contract dispute into a dangerous accusation that the
 13 contracting party posed a threat to national security.

14 The Department’s reaction was not only unjustified but also wildly disproportionate. The
 15 Department bypassed without considering—as required by statutory directive and by general
 16 prudence—the many ordinary tools the government has at its disposal to terminate or cabin its
 17 relationships with contractors. For instance, the government can terminate a contract for convenience
 18 when it is in its interest. *See* 48 C.F.R. §§ 49.101(b), 52.249-1–52.249-6. It can terminate a contract
 19 for cause in case of breach. *See id.* §§ 49.402-3, 52.212-4(m). It can direct changes “at any time” to the
 20 general scope of a contract, including the manner, method, or performance of the work, *id.* § 52.243-4,
 21 or suspend work on a contract, including to realign with its programs, *id.* §§ 42.1303, 52.242-15. It can
 22 also decline to award a contract based on a determination that a contractor or subcontractor is not
 23 responsible, *id.* §§ 9.103, 9.104-1(d), 9.104-4, and in more extreme cases can debar or suspend a
 24 contractor if in the public interest and with appropriate procedural safeguards, *id.* § 9.402(b). These are
 25 just a few of the many more proportionate authorities the Department can and routinely does leverage
 26 to bring an end to a current or potential future relationship with a contractor it deems untrustworthy or
 27 otherwise problematic—all of which stop far short of the extraordinary remedy deployed here.

1 The Department regularly utilizes the tools available to it to shape or limit its relationships with
 2 contractors, including when it deems a restriction on a contracted good or service to be at odds with its
 3 mission. Across every service branch, and for reasons as varied as cost overruns, shifting strategic
 4 priorities, technological overambition, or other performance failures, the Department has terminated
 5 contracts, or declined to exercise options under them, or deemed a contractor no longer responsible
 6 enough to work with the government. For example, in 2025, Secretary Hegseth announced over \$5
 7 billion in cancelled contracts, including nearly \$2 billion in cuts at the Defense Health Agency to
 8 contracts held by consulting firms, as part of a DOGE-driven effort to reduce overall spending at the
 9 Department.⁴ Sometimes, when priorities shift, it costs the Department less to terminate a major
 10 weapons systems contract than to complete it, even when a settlement must then be paid to a contractor.⁵
 11 On occasion, the Department will cancel high-dollar-value technology contracts if they “no longer
 12 [meet] the requirements to fill the D.O.D.’s capability gaps”—another way of framing the Department’s
 13 stated objections to Anthropic.⁶

14 Moreover, the government’s power over procurement has long been recognized by the Supreme
 15 Court. *See Perkins v. Lukens Steel Co.*, 310 U.S. 113, 127 (1940) (“Like private individuals and
 16 businesses, the Government enjoys the unrestricted power to produce its own supplies, to determine
 17 those with whom it will deal, and to fix the terms and conditions upon which it will make needed
 18 purchases.”); *Georgia v. President of the U.S.*, 46 F.4th 1283, 1292 n.5 (11th Cir. 2022) (observing that
 19 *Perkins*’ “propositions. . . hold true”). If the government is unhappy with a contractor, it can cease
 20 buying goods or services from them—and, as noted, it has a number of less-extreme statutory levers it
 21 can pull to achieve its aims. Here, the Department could simply have decided not to contract further

22
 23 ⁴ Nick Wakeman, *Pentagon Hits Accenture, Booz Allen and Deloitte with Contract Cancellations*,
 24 Wash. Tech. (Apr. 11, 2025), <https://www.washingtontechnology.com/contracts/2025/04/pentagon-hits-accenture-booz-allen-and-deloitte-contract-cancellations/404500/>. A separate \$1.4 billion reselling contract for Air Force enterprise cloud IT services was terminated around this time.

25 ⁵ Robert Brodsky, *GAO: Major Defense Contracts Cheaper to Cancel Than Continue*, Gov’t Exec.
 26 (Mar. 19, 2008), <https://www.govexec.com/defense/2008/03/gao-major-defense-contracts-cheaper-to-cancel-than-continue/26527>.

27 ⁶ Kate Conger & David E. Sanger, *Pentagon Cancels a Disputed \$10 Billion Technology Contract*, N.Y.
 28 Times (July 6, 2021), <https://www.nytimes.com/2021/07/06/technology/JEDI-contract-cancelled.html>.

1 with Anthropic, deeming the restrictions it imposed on its AI model no longer in the interests of the U.S.
 2 military. That is how the break-up of this kind of contractual relationship generally unfolds; the
 3 Department can't make a company change its product or its values, but it can decide, with few
 4 restrictions, that company or its product isn't right for the military.

5 Yet not a single less drastic measure appears to have been considered and deemed insufficient
 6 in this case, notwithstanding the unambiguous statutory mandate to determine whether “less intrusive
 7 measures” are “reasonably available,” 10 U.S.C. § 3252(b)(2)(B). That statutory language imposes a
 8 procedural and substantive safeguard against improper use of this weighty authority. As a procedural
 9 matter, the government must indicate, in some fashion, that it has considered less restrictive means—
 10 and no such indication exists here. As a substantive matter, that language unmistakably directs the
 11 Department to designate supply chain risks under this authority sparingly, judiciously, and only when
 12 absolutely necessary for reasons of national security—not for punitive reasons or to achieve, more
 13 dramatically, what it could already have achieved through the exercise of its standard procurement
 14 authorities.

15 The use of this designation under these circumstances, without considering any lesser
 16 alternatives, was extreme. In an ironic twist, however, the Pentagon's reported use of Mythos suggests
 17 Anthropic's technology may be too useful for the government to stay away for long. *See* Jake Bleiberg
 18 & Margi Murphy, *White House Moves to Give US Agencies Anthropic Mythos Access*, Bloomberg (Apr.
 19 16, 2026), [https://www.bloomberg.com/news/articles/2026-04-16/white-house-moves-to-give-us-](https://www.bloomberg.com/news/articles/2026-04-16/white-house-moves-to-give-us-agencies-anthropic-mythos-access)
 20 [agencies-anthropic-mythos-access](https://www.bloomberg.com/news/articles/2026-04-16/white-house-moves-to-give-us-agencies-anthropic-mythos-access). The government's continued interest in and use of Claude is all the
 21 more evidence that the supply-chain designation of Anthropic was pretextual. That it was not driven by
 22 any legitimate statutory considerations is obvious.

23 **B. PRETEXTUAL USE OF THIS SIGNIFICANT AUTHORITY UNDERMINES**
 24 **THE CREDIBILITY OF THE DEPARTMENT WITH INDUSTRY AND THE**
 25 **PUBLIC.**

26 The credibility of the Department and our Armed Forces depends on political neutrality and
 27 commitment to the rule of law. *See Greer v. Spock*, 424 U.S. 828, 839 (1976) (discussing the “American
 28 constitutional tradition of a politically neutral military establishment under civilian control”); *To*

1 *Support and Defend: Principles of Civilian Control and Best Practices of Civil-Military Relations*, War
 2 on the Rocks, para. 15 (Sept. 6, 2022) (open letter signed by Secretary Panetta) (“Military and civilian
 3 leaders must be diligent about keeping the military separate from partisan political activity.”). If the
 4 Department takes significant action that falls outside the bounds of the authority conferred by
 5 Congress—particularly where, as here, its decisions appear motivated by political retribution or
 6 animus—it risks upending public trust in the military and the decisions of its civilian leaders.

7 By undermining that critical trust, this supply chain risk designation could undermine America’s
 8 military supremacy and damage its ability to do its job. First, retaliatory and vindictive actions by
 9 Department leaders that appear to be motivated by partisan political disagreements undermine the
 10 public’s trust and confidence in the Pentagon’s civilian leaders and in the military as an institution.
 11 Public trust in the military is the foundation upon which any military action derives legitimacy. The
 12 fallout from the Anthropic designation will make the public less likely to trust the Department and the
 13 military overall, which will have ripple effects for recruitment and for Department morale.⁷ This is
 14 particularly concerning at present, since public confidence in the institution is already fragile; less than
 15 50% of Americans currently report a great deal of confidence in the military, down 21 points from 2018.
 16 See 2025 Reagan National Defense Survey, Ronald Reagan Inst. at 5 (Nov. 2025),
 17 [https://www.reaganfoundation.org/reagan-institute/centers/peace-through-strength/survey/2025-](https://www.reaganfoundation.org/reagan-institute/centers/peace-through-strength/survey/2025-reagan-national-defense-survey)
 18 [reagan-national-defense-survey](https://www.reaganfoundation.org/reagan-institute/centers/peace-through-strength/survey/2025-reagan-national-defense-survey).

19 Second, a pretextual supply chain risk designation undermines the public’s confidence in all
 20 future supply chain risk designations. This, in turn, undermines the very national security interests that
 21 section 3252 was designed to protect. If the government’s supply chain designations are viewed as
 22 suspect, private citizens and businesses may not follow the government’s lead in severing their personal
 23 and commercial connections to the companies and technologies that pose legitimate supply chain risks,

24
 25 ⁷ Cf. David Montgomery, *Many Americans Think AI Companies Should Be Able to Limit How The U.S.*
 26 *Military Uses Their Tools*, YouGov (Mar. 10, 2026), [https://yougov.com/en-us/articles/54285-many-](https://yougov.com/en-us/articles/54285-many-americans-think-ai-companies-should-be-able-to-limit-how-us-military-uses-tools-march-6-9-2026-economist-yougov-poll)
 27 [americans-think-ai-companies-should-be-able-to-limit-how-us-military-uses-tools-march-6-9-2026-](https://yougov.com/en-us/articles/54285-many-americans-think-ai-companies-should-be-able-to-limit-how-us-military-uses-tools-march-6-9-2026-economist-yougov-poll)
 28 [economist-yougov-poll](https://yougov.com/en-us/articles/54285-many-americans-think-ai-companies-should-be-able-to-limit-how-us-military-uses-tools-march-6-9-2026-economist-yougov-poll) (reporting on poll results finding that “Americans are more likely to say that AI
 companies should be able to restrict how their AI tools are used by the military than that the military
 should be able to use AI tools any way it wants (44% vs. 25%)”).

1 exposing industry and the public to threats from malicious actors and hostile foreign powers. For
 2 example, the Cybersecurity & Infrastructure Security Agency (“CISA”), which has warned about cyber
 3 and physical threats from hostile nation-states and nation-state sponsored entities, relies on partnerships
 4 with “critical infrastructure owners and operators nationwide.” *Nation State Threats*, CISA,
 5 <https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors>. CISA has
 6 explained that “it is critical to the nation’s safety and security that critical infrastructure owners and
 7 operators prepare for and adapt to changing conditions.” *Id.* But if private operators do not trust the
 8 government’s national security recommendations, they may not follow those recommendations in the
 9 future, leaving critical infrastructure vulnerable to hostile foreign actors.

10 Third, public companies that work with the military must have confidence that the government
 11 will be a reliable and trustworthy partner that adheres to the governing legal and regulatory frameworks
 12 when they enter into contracts with federal agencies. Unpredictability is bad for business. This is
 13 especially true for companies that develop emerging technologies, who may now hesitate before
 14 partnering with the federal government—and the military in particular—given the possibility that
 15 unforeseen disputes about technology use could drive the Department to impose crippling sanctions.
 16 The supply chain risk designation could, as a result, hinder the government’s ability to work with a
 17 range of different companies across different sectors, many of whom are key partners of agencies in
 18 helping them achieve their missions.

19 Fourth, and relatedly, the government could lose access to critical technologies. In early March,
 20 the Information Technology Industry Council, a technology industry group whose members include
 21 Nvidia, Amazon, and Apple, expressed exactly these concerns to Secretary Hegseth, lamenting that
 22 misuse of supply-chain designation authorities could “undermine the government’s access to the best-
 23 in-class products and services from American companies that serve all agencies and components of the
 24 federal government.”⁸ The Department could find itself cut off from the most capable AI systems
 25 precisely as such systems become most consequential to military operations. It is no surprise, then, that

26
 27 ⁸ See Karen Freifeld, *Big Tech Group Tells Pentagon’s Hegseth They Are ‘Concerned’ About Anthropic*
 28 *Supply-Chain Risk Designation*, Reuters (Mar. 4, 2026), <https://www.reuters.com/business/retail-consumer/big-tech-group-tells-pentagons-hegseth-they-are-concerned-about-declaring-2026-03-04>.

1 public reporting confirms that “Pentagon staffers, former officials and IT contractors who work closely
 2 with the U.S. military say they are reluctant to give up Anthropic’s AI tools, which they view as superior
 3 to alternatives.” Mike Stone et al., *Hegseth Wants Pentagon to Dump Anthropic’s Claude, But Military*
 4 *Users Say It’s Not So Easy*, Reuters (Mar. 19, 2026), [https://www.reuters.com/business/hegseth-wants-](https://www.reuters.com/business/hegseth-wants-pentagon-dump-anthropics-claude-military-users-say-its-not-so-easy-2026-03-19/)
 5 [pentagon-dump-anthropics-claude-military-users-say-its-not-so-easy-2026-03-19/](https://www.reuters.com/business/hegseth-wants-pentagon-dump-anthropics-claude-military-users-say-its-not-so-easy-2026-03-19/).

6 The military maintains its technological supremacy through partnerships with America’s
 7 businesses that enable it to leverage American ingenuity and technological innovation. Undermining
 8 this trust and the partnerships that rely on it jeopardizes America’s national security by cutting off
 9 military personnel from critical technologies and the companies supplying and developing those
 10 technologies.

11 This is all the more damaging as powerful new AI systems emerge with significant national
 12 security applications. Anthropic’s new model, Mythos, is reportedly able to identify and exploit and
 13 also patch zero-day cybersecurity vulnerabilities in major operating systems and web browsers, making
 14 it a uniquely valuable tool for national defense. See Nicholas Carlini et al., *Assessing Claude Mythos*
 15 *Preview’s Cybersecurity Capabilities*, Anthropic Red Team (Apr. 7, 2026),
 16 <https://red.anthropic.com/2026/mythos-preview/>; see also *Our Evaluation of Claude Mythos Preview’s*
 17 *Cyber Capabilities*, UK AI Sec. Inst.: Blog (Apr. 13, 2026), [https://www.aisi.gov.uk/blog/our-](https://www.aisi.gov.uk/blog/our-evaluation-of-claude-mythos-previews-cyber-capabilities)
 18 [evaluation-of-claude-mythos-previews-cyber-capabilities](https://www.aisi.gov.uk/blog/our-evaluation-of-claude-mythos-previews-cyber-capabilities). As of late May 2026, Anthropic and roughly
 19 50 partners have used Mythos to “find more than ten thousand high- or critical-severity vulnerabilities
 20 across the most systemically important software in the world.” *Project Glasswing: An Initial Update*,
 21 Anthropic (May 22, 2026), <https://www.anthropic.com/research/glasswing-initial-update>. The supply
 22 chain designation of Anthropic threatens to make it difficult for the government to take full advantage
 23 of this new model to address its vulnerabilities at a sensitive moment for national defense. What’s more,
 24 critical infrastructure providers who also contract with the government are highly likely to be reluctant
 25 to engage with Anthropic to test Mythos’s capabilities, over fears that association with the company
 26 will damage their competitiveness for future contracts with the federal government. The Department’s
 27 actions are therefore actively preventing critical infrastructure owners and operators, including in the
 28

1 military, from strengthening their cyber defenses through the development and deployment of Mythos—
 2 thereby undermining the credibility and safety of government systems at a time when the United States
 3 is actively engaged in hostilities with a foreign nation and other non-state actors.

4 **II. IMPROPER DESIGNATION OF ANTHROPIC AS A SUPPLY CHAIN RISK**
 5 **THREATENS THE U.S.’S MILITARY AND ECONOMIC ADVANTAGE AT A**
 6 **PIVOTAL MOMENT IN U.S.–CHINA TECHNOLOGICAL COMPETITION.**

7 The United States is engaged in a high-stakes AI competition with China, the outcome of which
 8 will have profound consequences for American military and economic strength. The nation that leads
 9 in AI will also gain substantial advantages on the battlefield, as “frontier AI” systems—the most cutting-
 10 edge AI models—are increasingly capable of accelerating intelligence collection and analysis,
 11 supporting weapons development, and conducting offensive and defensive cyber operations. Mythos
 12 provides a case in point: The UK AI Security Institute, a leading British government institution
 13 dedicated to evaluating the safety and security of advanced AI models, performed an independent
 14 evaluation of Mythos’s cyber capabilities and found that it was able to “execute multi-stage attacks on
 15 vulnerable networks and discover and exploit vulnerabilities autonomously.” *Our Evaluation of Claude*
 16 *Mythos Preview’s Cyber Capabilities*, UK AI Sec. Inst.: Blog (Apr. 13, 2026),
 17 <https://www.aisi.gov.uk/blog/our-evaluation-of-claude-mythos-previews-cyber-capabilities>. The U.S.
 18 military has already reportedly used earlier Claude models to plan and execute sensitive military
 19 operations. In the hands of U.S. adversaries, such capabilities present a frightening proposition. Beyond
 20 military advantages, the winner of the AI race may also benefit from significant gains in economic
 21 productivity and related GDP growth.

22 China understands the stakes and has invested accordingly. *See* Kyle Chan et al., *Full Stack:*
 23 *China’s Evolving Industrial Policy for AI*, RAND (June 26, 2025) (noting that “China wants to become
 24 the global leader in artificial intelligence (AI) by 2030” and is “deploying industrial policy tools across
 25 the full AI technology stack, from chips to applications,” to achieve that goal). Although the United
 26 States remains ahead in technical capabilities, Beijing is catching up. For the past few years, Chinese
 27 AI models have been just half a year behind the top U.S. models on average. *See* Luke Emberson,
 28 *Chinese AI Models Have Lagged the US Frontier by 7 Months on Average Since 2023*, Epoch AI (Jan.

2, 2026). A Chinese lead in frontier AI would give Beijing a decisive advantage in military planning, cyber operations, and intelligence analysis at precisely the moment those capabilities are becoming most consequential.

The United States cannot outcompete China by playing by Beijing's rules. Washington's advantage comes not from out-spending or out-planning Beijing, but from maintaining a flourishing private sector, governed by stable and predictable rules, that drive technological innovation at scale. *See* Fatima Faisal Khan, *The Missing Middle*, Inst. for Sec. + Tech. at 32-33 (Oct. 2025) (the United States maintains "clear leadership in artificial intelligence" because "[t]ransparent governance attracts the global capital that China's opacity repels"). China has enduring strengths in AI talent and energy infrastructure, and is pouring resources into its AI ecosystem. What China cannot replicate, however, is the stability of the relationship in the United States between the public and private sectors, which allows companies to innovate, commercialize, and grow without fear of interference or reprisal. *See* Scott Singer & Matt Sheehan, *China's AI Policy at the Crossroads: Balancing Development and Control in the DeepSeek Era*, Carnegie Endowment for Int'l Peace (July 17, 2025) (noting that China has exercised strict control over its AI sector by "systematically reassert[ing] its power over China's leading technology companies through antitrust investigations, stricter regulations, record-breaking fines, and, in some cases, the acquisition of board seats by state entities"). This stability and predictability is why the world's leading frontier AI models—including Anthropic's Claude—are American. It is also why American AI systems are the technology of choice for allied governments and global companies. The relationship between the Department and the private sector is not only vital to ensuring that American AI development outpaces Chinese AI development; it is also key to translating private-sector innovations into economic and battlefield advantages.

Moreover, when the Department deploys its substantial authorities to punish a leading technology company, it signals that doing business in the United States is risky, and that frontier AI labs should take their business elsewhere. And, at the same time, the designation could accelerate efforts by foreign countries to diversify away from American AI, weakening the country's AI ecosystem on which its modern-day military and economic dominance depend. If it appears that Silicon Valley is at the

mercy of the U.S. government, it may create an environment in which foreign countries are more likely to adopt Chinese AI or build their own sovereign capabilities—an outcome that would run directly counter to U.S. national security interests. *See, e.g.,* Pablo Chavez, *The Sovereignty Gap in U.S. AI Statecraft*, Lawfare (Feb. 16, 2026), <https://www.lawfaremedia.org/article/the-sovereignty-gap-in-u.s.-ai-statecraft>; Dean Ball, *Clawed*, Hyperdimensional (Mar. 2, 2026), <https://www.hyperdimensional.co/p/clawed>. The Department’s supply chain risk designation of Anthropic is a live demonstration of what foreign AI purchasers fear: that reliance on American AI exposes them to the shifting and mercurial impulses of the U.S. Executive Branch.

Much damage has already been done. If Anthropic’s designation as a supply chain risk is not reversed, it is likely that Washington will come to regret its self-harm in the most important geopolitical competition of our age.

CONCLUSION

For the foregoing reasons, the Court should grant Anthropic’s Motion for Summary Judgement.

DATED: June 26, 2026

s/Todd C. Toral

TODD C. TORAL
MATTHEW KLAPPER*
JENNER & BLOCK LLP
*Counsel for Amici Curiae Leon Panetta and the
Institute for Security and Technology*

**Pro hac vice forthcoming.*
E-mail: TToral@jenner.com
MKlapper@jenner.com

Counsel for Amici Curiae Leon Panetta and the Institute for Security and Technology