

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

THE PROTECT DEMOCRACY PROJECT,
INC.,

Plaintiff,

v.

OFFICE OF THE NATIONAL CYBER
DIRECTOR, OFFICE OF SCIENCE AND
TECHNOLOGY POLICY, U.S.
DEPARTMENT OF COMMERCE,
BUREAU OF INDUSTRY AND SECURITY,
and U.S. DEPARTMENT OF THE
TREASURY,

Defendants.

Case No. 1:26-cv-03064

MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT OF
PLAINTIFF'S MOTION FOR A PRELIMINARY INJUNCTION

Justin Florence (D.D.C. Bar No. 988953)
Deana K. El-Mallawany*
THE PROTECT DEMOCRACY PROJECT, INC.
2020 Pennsylvania Avenue, NW, #163
Washington, D.C. 20006
Telephone: (202) 579-4582
Facsimile: (929) 777-8428
justin.florence@protectdemocracy.org
deana.elmallawany@protectdemocracy.org

Michael P. Abate
(D.D.C. Bar No. MD28077)
(D.C. Bar No. 1023343)
Burt A. ("Chuck") Stinson*
KAPLAN JOHNSON ABATE & BIRD LLP
710 W. Main St., 4th Floor
Louisville, KY 40202
Telephone: (502) 540-8280
mabate@kaplanjohnsonlaw.com

Counsel for Plaintiff

**Motion for Pro Hac Vice Forthcoming*

TABLE OF CONTENTS

INTRODUCTION	1
BACKGROUND	3
I. The Executive Branch Has Asserted New, Undisclosed Authority Over Frontier AI Models.....	3
II. August 2026 Reporting Confirms the Framework Has Been Finalized in Secret.	5
III. GOLD EAGLE Depends on Statutory Protections Set to Expire on September 30, 2026, Which Are Actively Being Debated in Congress.	6
IV. Protect Democracy Submitted Narrow FOIA Requests, and Defendants Have Not Substantively Responded.	8
ARGUMENT	10
I. This Court Has Jurisdiction To Grant The Requested Relief.....	10
II. Plaintiff is Entitled to a Preliminary Injunction	10
A. Plaintiff is Likely to Succeed on the Merits.....	12
1. Plaintiff is Entitled to Expedited Processing of their FOIA Requests Because There is a Compelling Need to Inform the Public About the Details of the Government’s Frontier AI Framework and the Legal Basis of the GOLD EAGLE Program.....	12
2. Plaintiff is Entitled to Production or a Response “as Soon as Practicable”	22
B. Plaintiff Will Be Irreparably Harmed Absent the Requested Relief.....	23
C. The Requested Relief Will Not Burden Others’ Interests	25
D. The Public Interest Favors the Requested Relief	26
CONCLUSION.....	28

TABLE OF AUTHORITIES

Cases

<i>ACLU v. U.S. Dep’t of Justice</i> , 321 F. Supp. 2d 24 (D.D.C. 2004)	10
<i>Al-Fayed v. CIA</i> , 254 F.3d 300 (D.C. Cir. 2001)	10, 12, 15, 16
<i>American Oversight v. U.S. Department of State</i> , 414 F. Supp. 3d 182 (D.D.C. 2019).....	11
<i>Brennan Ctr. for Just. at NYU Sch. of L. v. Dep’t of Commerce</i> , 498 F. Supp. 3d 87 (D.D.C. 2020)	passim
<i>Center for Public Integrity v. DOD</i> , 411 F. Supp. 3d 5 (D.D.C. 2019)	12, 27
<i>Citizens for Resp. & Ethics in Washington v. U.S. Dep’t of Just.</i> , 826 F. Supp. 3d 73 (D.D.C. 2026)	11, 23
<i>Citizens for Responsibility & Ethics in Washington v. Fed. Election Comm’n</i> , 711 F.3d 180 (D.C. Cir. 2013)	22
<i>Ctr. to Prevent Handgun Violence v. U.S. Dep’t of Treasury</i> , 49 F. Supp. 2d 3 (D.D.C. 1999)	26
<i>Democracy Forward Found. v. Off. of Mgmt. & Budget</i> , 780 F. Supp. 3d 61 (D.D.C. 2025)	16
<i>Elec. Frontier Found. v. Office of Dir. of Nat. Intelligence</i> , No. C 07-5278, 2007 WL 4208311 (N.D. Cal. Nov. 27, 2007)	18, 24
<i>Elec. Priv. Info. Ctr. v. Nat’l Sec. Comm’n on A.I.</i> , 419 F. Supp. 3d 82 (D.D.C. 2019)	15, 23
<i>Elec. Privacy Info. Ctr. v. Presidential Advisory Comm’n on Election Integrity</i> , 266 F. Supp. 3d 297 (D.D.C. 2017)	23
<i>Electronic Privacy Info. Ctr. v. U.S. Dep’t of Just.</i> , 416 F. Supp. 2d 30 (D.D.C. 2006)	passim
<i>Jacksonville Port Auth. v. Adams</i> , 556 F.2d 52 (1977).....	26
<i>Leadership Conference on Civil Rights v. Gonzales</i> , 404 F. Supp. 2d 246 (D.D.C. 2005).....	11, 13, 17
<i>Legion LegalTech Corp. v. United States</i> , No. 1:26-cv-02225 (D.D.C. filed June 23, 2026).....	4
<i>Open Soc’y Justice Initiative v. CIA</i> , 2019 WL 3561889 (S.D.N.Y. Aug. 6, 2019)	13
<i>Payne Enters., Inc. v. United States</i> , 837 F.2d 486 (D.C. Cir. 1988)	22

<i>Protect Democracy Project, Inc. v. U.S. Dep’t of Def.</i> , 263 F. Supp. 3d 293 (D.D.C. 2017)	13, 17, 24, 26
<i>Protect Democracy Project, Inc. v. United States Dep’t of Just.</i> , 498 F. Supp. 3d 132 (D.D.C. 2020)	13
<i>U.S. Dep’t of Justice v. Reporters Comm. for Freedom of the Press</i> , 489 U.S. 749 (1989)	10, 26
<i>Washington Post v. U.S. Dep’t of Homeland Sec.</i> , 459 F. Supp. 2d 61 (D.D.C. 2006)	11, 24

Statutes and Legislative Materials

5 U.S.C. § 552(a)(3)(A)	28
5 U.S.C. § 552(a)(4)(B)	12
5 U.S.C. § 552(a)(6)(E)	passim
H.R. Rep. 104-795, 26, 1996 U.S.C.C.A.N. 3448, 3469	19
Cong. Research Serv., IF12959, <i>The Cybersecurity Information Sharing Act of 2015: Expiring Provisions</i> (May 8, 2026)	8, 10
Cong. Research Serv., IF13197, <i>Cyber and Artificial Intelligence Provisions in the FY2026 National Defense Authorization Act</i> (NDAA) (July 2026)	8

Regulations

15 C.F.R. § 4.6(f)	16, 19
31 C.F.R. § 1.4(e)	16
32 C.F.R. § 2200.6(d)(ii)	16
32 C.F.R. § 2402.6(d)	17
<i>Implementing the Freedom of Information Act and Privacy Act</i> , 91 Fed. Reg. 15,932 (Mar. 31, 2026)	17

Executive Orders and Announcements

Executive Order 14409, <i>Promoting Advanced Artificial Intelligence Innovation and Security</i> (the “AI Security EO”), 91 Fed. Reg. 34,565 (June 5, 2026)	4, 7, 20
White House, <i>White House Launches Gold Eagle Initiative for Unprecedented</i> <i>Cybersecurity Vulnerability Coordination</i> (July 14, 2026)	7, 20

Other Materials

Alan Z. Rozenshtein, <i>A Kill Switch for Frontier AI, Lawfare</i> (June 15, 2026)	5
---	---

Ashley Capoot, <i>Anthropic Says Trump Admin Has Lifted Export Controls on Claude Fable 5 and Mythos 5,</i> CNBC (June 30, 2026).....	5
Ashley Capoot, <i>OpenAI Limits New AI Models to ‘Trusted Partners’ at Request of U.S. Government,</i> CNBC (June 26, 2026).....	5
<i>Brief independent investigation of agents’ behavior, reasoning and collaboration in the OpenAI / Hugging Face hacking incident (Aug. 26, 2026)</i>	25
Eric Geller, <i>AI-Powered Vulnerability Clearinghouse Faces Deep Skepticism, Major Challenges,</i> Cybersecurity Dive (Aug. 19, 2026).....	10
Jake Taylor, <i>AI Systems Are Getting More Powerful. The Ability to Verify Must Keep Pace,</i> Tech Policy Press (Aug. 25, 2026)	25
Maria Curi, <i>Scoop: Inside Trump’s AI framework (Aug. 4, 2026).....</i>	6
Maria Curi, <i>White House Excludes Open Models from AI Framework,</i> Axios (Aug. 4, 2026)	6
Maria Curi, <i>White House Finalizes AI Framework Behind Closed Doors,</i> Axios (Aug. 3, 2026)	6
Martin Matishak, <i>Extension of CISA 2015 Info-Sharing Protections Passes as Part of House’s Defense Bill,</i> The Record (July 22, 2026)	2, 10
Miranda Nazzaro, <i>Trump administration’s closed-door AI framework catches tech policy sector off guard</i> (Aug. 10, 2026).....	6
Noah Barger, <i>The Clock Is Ticking on U.S. Cybersecurity,</i> Info. Tech. Indus. Council TechWonk Blog (July 31, 2026).....	3, 10
<i>Pacing the Frontier,</i> www.pacingthefrontier.com.....	26, 32
<i>Senate Approves Bill to Fund Government into December, but House Support Remains Uncertain,</i> CBS News (Aug. 8, 2026)	9
<i>Senate Stopgap Extends Key Cyber Authorities,</i> TMF, Federal News Network (Aug. 2026).....	9
Suzanne Smalley, <i>Trump Administration Unveils AI-Supported Clearinghouse for Cyber Vulnerabilities,</i> The Record (July 15, 2026)	2, 8

INTRODUCTION

This case concerns four time-sensitive Freedom of Information Act (“FOIA”) requests for records regarding the federal government’s oversight of frontier artificial intelligence models.

Since June 2026, the Executive Branch has taken an extraordinary role in deciding which companies may release advanced AI models, on what terms, and which customers and governments may access them first. It has done so without any apparent statutory authorization, and it has disclosed almost nothing to the public about how those decisions are made or who is making them. In June 2026, for example, Defendant the Bureau of Industry and Security gave a leading AI developer ninety minutes to comply with a directive resulting in the worldwide suspension of its most advanced models, invoking export-control authority that had never before been used for a comparable purpose. The government has since finalized a framework for deciding which companies get advance access to new AI models before they are ever released to the public, largely behind closed doors. In addition, on July 14, 2026, the administration announced a multi-agency clearinghouse called GOLD EAGLE that coordinates with AI companies to identify and fix cybersecurity vulnerabilities using frontier AI tools.

Plaintiff Protect Democracy Project, Inc. (“Protect Democracy”) submitted four FOIA requests to identify the legal authority, the participants, and the operative terms of two of these initiatives: the voluntary “pre-release review framework” established under Executive Order 14409, and the “GOLD EAGLE” AI-cybersecurity clearinghouse announced on July 14, 2026. Protect Democracy limited each request to narrow categories of records concerning the framework’s text, its legal basis, and the identities of participating companies for each program. It deliberately made these requests targeted, so that Defendants could comply quickly and this litigation could be avoided. And given the important stakes of this request, it sought expedition.

Three weeks later, no Defendant has granted expedition, ruled on Protect Democracy’s fee

waivers, or produced a single record. Only one defendant has addressed the requests’ substance at all: Defendant Office of the National Cyber Director (“ONCD”), whose answer that it “will respond ... in more than 20 days due to limited resources” is an effective denial of expedition, which Protect Democracy has appealed (without response to date).

Time is of the essence for three independent reasons. First, GOLD EAGLE’s information-sharing function depends on liability and disclosure protections under the Cybersecurity Information Sharing Act of 2015 (“CISA 2015”) that are set to sunset on September 30, 2026 absent congressional reauthorization,¹ and Congress’s path to reauthorization is contested and narrowing. A senior administration official has publicly acknowledged that, absent that reauthorization, “this effort is fundamentally challenged.” Suzanne Smalley, *Trump Administration Unveils AI-Supported Clearinghouse for Cyber Vulnerabilities*, *The Record* (July 15, 2026).² Industry groups have separately warned that CISA 2015’s deadline falls on the same date as the federal government’s funding deadline and have urged Congress to extend the statute before the end of September. Martin Matishak, *Extension of CISA 2015 Info-Sharing Protections Passes as Part of House’s Defense Bill*, *The Record* (July 22, 2026).³

Second, new frontier models are moving through the secret pre-release review now, amid heightened public concern about the efficacy of pre-release review in light of recent incidents manifesting the risks of new models. Each release that passes through the framework is an

¹ Cybersecurity Information Sharing Act of 2015, Pub. L. No. 114-113, div. N, tit. I, 129 Stat. 2936 (2015), extended by Consolidated Appropriations Act, 2026, Pub. L. No. 119-75, § 5008 (2026) (extending sunset to Sept. 30, 2026); Cong. Research Serv., IF13197, *Cyber and Artificial Intelligence Provisions in the FY2026 National Defense Authorization Act (NDAA)* (July 2026) (noting CISA 2015’s reauthorization was not included in the FY2026 NDAA).

² Available at <https://therecord.media/gold-eagle-cybersecurity-vulnerabilities-clearinghouse>.

³ Available at <https://therecord.media/cisa-2015-extension-passes-house-ndaa>; Noah Barger, *The Clock Is Ticking on U.S. Cybersecurity*, Info. Tech. Indus. Council TechWonk Blog (July 31, 2026), <https://www.itic.org/news-events/techwonk-blog/the-clock-is-ticking-on-us-cybersecurity>.

application of undisclosed rules that can never be publicly examined in time to matter.

Third, the constituencies who must act on this information—including a state legislature facing end-of-session votes on and implementation of AI standards formulated without seeing the federal framework, investors and businesses making irreversible commitments under rules they cannot see, and the independent evaluators who are seeking to analyze the same vulnerabilities—face their own imminent decisions, as the accompanying declarations detail. If the requested records are not produced on the requested timeline, Protect Democracy and the public will permanently lose the opportunity to inform Congress’s evaluation of GOLD EAGLE, California’s AI standards legislation, safety monitors’ oversight of emerging frontier AI models and the risks they pose, and investment and business decisions of those who rely on transparent information about these models. A later merits judgment, however favorable, cannot restore that opportunity.

The relief sought is correspondingly modest. The framework exists in final form and appears to be unclassified based on the government’s reported acknowledgment and disclosure to private companies. Protect Democracy asks only that Defendants be ordered to grant expedited processing, conduct an adequate search, and produce all responsive, non-exempt records as soon as practicable. Plaintiff proposes a schedule where Defendants must complete their searches by September 15, 2026 and provide any responsive records (or justify its withholdings) no later than September 30, 2026—in other words, before the window in which these records can inform the decisions they concern closes.

BACKGROUND

I. The Executive Branch Has Asserted New, Undisclosed Authority over Frontier AI Models.

On June 2, 2026, the President signed Executive Order 14409, *Promoting Advanced Artificial Intelligence Innovation and Security* (the “AI Security EO”), 91 Fed. Reg. 34,565 (June

5, 2026). The AI Security EO creates a process for determining when an AI model qualifies as a “covered frontier model.” Exec. Order No. 14409, § 3(a). It also calls for the creation of a “voluntary framework with AI developers” under which the federal government would receive up to thirty days of exclusive access to a covered model before its release, and under which certain “trusted partners” would receive early access to the model before a general release. *Id.* § 3(b).

Under the AI Security EO, only the benchmarking methodology used to determine whether a model qualifies as a “covered frontier model” is to be classified. The EO does not contemplate that the framework described in Section 3(b)—including the thirty-day pre-release access period and the process for selecting “trusted partners”—would be classified.

Ten days later, on June 12, 2026, Defendant BIS gave the AI developer Anthropic PBC ninety minutes to comply with a directive resulting in the suspension of worldwide access to two of its models, Claude Fable 5 and Claude Mythos 5. BIS invoked export-control authority that had not previously been used to control model access. Complaint at 2, *Legion LegalTech Corp. v. United States*, No. 1:26-cv-02225 (D.D.C. filed June 23, 2026); Alan Z. Rozenshtein, *A Kill Switch for Frontier AI*, *Lawfare* (June 15, 2026).⁴ Access to Mythos 5 was later restored, but at first only for an undisclosed set of “trusted partner” entities. BIS lifted the export controls entirely on June 30, 2026. Ashley Capoot, *Anthropic Says Trump Admin Has Lifted Export Controls on Claude Fable 5 and Mythos 5*, *CNBC* (June 30, 2026).⁵ Around the same time, and without any public order, OpenAI Group PBC agreed to limit distribution of its own forthcoming models to government-vetted partners, at the government’s request. Ashley Capoot, *OpenAI Limits New AI Models to ‘Trusted Partners’ at Request of U.S. Government*, *CNBC* (June 26, 2026).⁶ Neither the

⁴ Available at <https://www.lawfaremedia.org/article/a-kill-switch-for-frontier-ai>.

⁵ Available at <https://www.cnbc.com/2026/06/30/anthropic-says-trump-admin-has-lifted-export-controls-on-claude-fable-5-and-mythos-5.html>.

⁶ Available at <https://www.cnbc.com/2026/06/26/openai-limits-new-ai-models-to-trusted->

identity of any trusted partner, nor the criteria by which that status is granted or withheld, has been made public.

II. August 2026 Reporting Confirms the Framework Has Been Finalized in Secret.

On August 3, 2026, Axios reported that the pre-release review framework contemplated by the AI Security EO had in fact been finalized days earlier. Maria Curi, *White House Finalizes AI Framework Behind Closed Doors*, Axios (Aug. 3, 2026).⁷ The White House does not intend to release it publicly, however. As one unnamed White House official put it: “Just because things are unclassified that doesn’t mean we are going to broadcast them to everyone.” *Id.*

According to multiple sources briefed on White House meetings, the framework defines a covered frontier model as a closed-source system with advanced capabilities that could pose a risk to national security. Maria Curi, *Scoop: Inside Trump’s AI framework* (Aug. 4, 2026).⁸ It apparently does not clearly define either standard, however. Open-source models are excluded from the framework altogether, and the framework does not restrict an open model once it has been released. *Id.*

Public reporting describes a thirty-day government review period during which company employees would be restricted from accessing a covered model. *Id.* The model would be held in a high-security environment, and access to it would be logged. The review itself would be conducted by officials across several parts of the administration rather than a single office or agency. *Id.*

partners-request-us-government.html.

⁷ Available at <https://www.axios.com/2026/08/03/white-house-finalizes-ai-framework-behind-closed-doors>; see also Maria Curi, *White House Excludes Open Models from AI Framework*, Axios (Aug. 4, 2026), <https://www.axios.com/2026/08/04/white-house-ai-framework-under-wraps>.

⁸ Available at <https://www.axios.com/2026/08/04/trump-ai-framework-open-models>; see also Miranda Nazzaro, *Trump administration’s closed-door AI framework catches tech policy sector off guard* (Aug. 10, 2026), <https://thehill.com/policy/technology/6017847-trump-closed-door-ai-framework-withheld/>.

The White House convened meetings with select industry participants to review the framework on August 4, while companies that were not invited—like the public—remain in the dark about the framework’s contents. The White House also refuses to disclose which “trusted partners” (including whether any foreign government) will receive early access to new models. *Id.*

III. GOLD EAGLE Depends on Statutory Protections Set to Expire on September 30, 2026, Which Are Actively Being Debated in Congress.

The AI Security EO also directs the Secretary of the Treasury, in consultation with the National Cyber Director, the Secretary of War, and the Secretary of Homeland Security, to “form an AI cybersecurity clearinghouse, in voluntary collaboration with the AI industry and operators of critical infrastructure,” to coordinate the discovery, validation, and remediation of software vulnerabilities. AI Security EO § 2(d). The government announced that clearinghouse, GOLD EAGLE, on July 14, 2026. White House, *White House Launches Gold Eagle Initiative for Unprecedented Cybersecurity Vulnerability Coordination* (July 14, 2026).⁹ It did not, however, identify which companies are participating in GOLD EAGLE, the terms of that participation, or the legal authority under which the clearinghouse operates.

It appears that GOLD EAGLE’s information-sharing function between AI companies depends on liability and disclosure protections that already exist under CISA 2015. *Id.* A senior administration official has confirmed that GOLD EAGLE’s continued operation is made possible by CISA 2015 and that, without reauthorization, “this effort is fundamentally challenged.” Suzanne Smalley, *Trump Administration Unveils AI-Supported Clearinghouse for Cyber Vulnerabilities*, *The Record* (July 15, 2026).¹⁰

CISA 2015 is a controversial enactment that has intermittently lapsed. It was enacted with

⁹ Available at <https://www.whitehouse.gov/releases/2026/07/white-house-launches-gold-eagle-initiative-for-unprecedented-cybersecurity-vulnerability-coordination/>.

¹⁰ Available at <https://therecord.media/gold-eagle-cybersecurity-vulnerabilities-clearinghouse>.

a ten-year sunset. It first lapsed on September 30, 2025, was restored after a six-week gap in coverage, and has since been extended twice for short periods, most recently through the Consolidated Appropriations Act, 2026, which pushed the sunset to September 30, 2026. Cong. Research Serv., IF12959, *The Cybersecurity Information Sharing Act of 2015: Expiring Provisions* (May 8, 2026).¹¹ Reauthorization was not included in the FY2026 National Defense Authorization Act, the vehicle that has carried it in past years. Cong. Research Serv., IF13197, *Cyber and Artificial Intelligence Provisions in the FY2026 National Defense Authorization Act (NDAA)* (July 2026).¹²

Instead, CISA reauthorization is currently working its way on parallel tracks through the annual defense-policy and appropriations processes. On the defense-policy track, the House included a ten-year extension, styled the Widespread Information Management for the Welfare of Infrastructure and Government Act, in its version of the fiscal year 2027 National Defense Authorization Act. The Senate's counterpart bill does not yet contain a matching provision, and Senator Rand Paul, who chairs the committee with jurisdiction over the reauthorization, has said he will not let it advance without unrelated policy changes.

On the appropriations side, the Senate passed a continuing resolution on August 8, 2026 that would fund the federal government through December 11, 2026 and would extend CISA 2015 through that date. *See Senate Stopgap Extends Key Cyber Authorities, TMF*, Federal News Network (Aug. 2026).

The House of Representatives passed its own continuing resolution before adjourning for the August recess; that bill would fund the government only through December 4, 2026, and does not include a corresponding extension of CISA 2015. *See Senate Approves Bill to Fund*

¹¹ Available at https://www.congress.gov/crs_external_products/IF/HTML/IF12959.html.

¹² Available at <https://www.congress.gov/crs-product/IF13197>.

Government into December, but House Support Remains Uncertain, CBS News (Aug. 8, 2026).

The House returned from recess on August 31, 2026, and as of this filing was expected to pass the Senate version later that week. If signed by the President, the continuing resolution would extend CISA 2015 for just over two months, to early December. Thus the debate over CISA 2015 will continue with urgency regardless of what happens to the continuing resolution in the coming days.

Industry groups have pressed Congress to act on the statute more broadly, beyond extension of the sunseting information-sharing authority, before the end of September.¹³ Current CISA 2015 does not specifically address artificial intelligence, and commentators have identified whether and how to extend the statute's protections to AI-assisted information sharing, the very activity GOLD EAGLE performs, as an open question for this reauthorization.¹⁴ Moreover, independent reporting in the past several weeks has separately raised questions about GOLD EAGLE's operation, including specific questions about Treasury's oversight of the clearinghouse and the funding of its central technology system. Eric Geller, *AI-Powered Vulnerability Clearinghouse Faces Deep Skepticism, Major Challenges*, Cybersecurity Dive (Aug. 19, 2026).¹⁵

IV. Protect Democracy Submitted Narrow FOIA Requests, and Defendants Have Not Substantively Responded.

On August 7, 2026, Protect Democracy submitted substantively identical FOIA requests to each Defendant.¹⁶ Compl., Ex. A. Each request sought the same three categories of records for both the pre-release review framework and GOLD EAGLE: (1) the complete text of the relevant

¹³ Martin Matishak, *Extension of CISA 2015 Info-Sharing Protections Passes as Part of House's Defense Bill*, The Record (July 22, 2026), <https://therecord.media/cisa-2015-extension-passes-house-ndaa>; Noah Barger, *The Clock Is Ticking on U.S. Cybersecurity*, Info. Tech. Indus. Council TechWonk Blog (July 31, 2026), <https://www.itic.org/news-events/techwonk-blog/the-clock-is-ticking-on-us-cybersecurity>.

¹⁴ Cong. Research Serv., IF12959, *supra*.

¹⁵ Available at <https://www.cybersecuritydive.com/news/ai-vulnerability-clearinghouse-us-government-challenges/827710/>.

¹⁶ Deana El-Mallawany, FOIA Requests to ONCD, OSTP, BIS, and Treasury (Aug. 7, 2026)

framework or clearinghouse terms, (2) records identifying the companies participating in or considered for it, and (3) records identifying the legal authority under which it operates.

Each request also sought expedited processing under 5 U.S.C. § 552(a)(6)(E), and the corresponding regulation of the agency to which it was addressed, on the ground that Protect Democracy is primarily engaged in disseminating information and that there is an urgency to inform the public concerning actual or alleged Federal Government activity. *Id.* § 552(a)(6)(E)(v). Each request also sought a fee waiver on public-interest grounds and certified, as required, the truth of the statements made in support of the request.

Of the four Defendants, only ONCD responded within the ten calendar days that FOIA and ONCD's own regulations allow for a decision on expedited processing. That response, dated August 17, 2026, stated that ONCD "will respond to your FOIA request in more than 20 days due to limited resources to search, locate, and review the records you seek."¹⁷ Compl., Ex. B. Protect Democracy treats that response as a denial of expedited processing and timely appealed it on August 19, 2026, exhausting its administrative remedies as to ONCD.¹⁸ Compl., Ex. C.

BIS, and Treasury did not acknowledge the requests within ten calendar days and have therefore constructively exhausted Protect Democracy's administrative remedies with respect to expedited processing under 5 U.S.C. § 552(a)(6)(C)(i). The twenty-business-day deadline for a substantive response to the ONCD, BIS, and Treasury requests will elapse on September 4, 2026.

Protect Democracy originally sent its request to Defendant OSTP on August 7, 2026, at the same time it requested the information from the other three agencies. On August 17, Defendant OSTP informed Plaintiff that its original FOIA request needed to be served on the agency by other means. Plaintiff redelivered its FOIA request to OSTP on August 25. Compl., Ex. D. As a result,

¹⁷ Letter from ONCD to Deana El-Mallawany (Aug. 17, 2026)

¹⁸ Administrative Appeal to ONCD (Aug. 19, 2026)

the periods described in 5 U.S.C. § 552(a)(6) with respect to OSTP now run from August 25, 2026.

No Defendant has produced a single responsive record.

ARGUMENT

I. This Court Has Jurisdiction To Grant The Requested Relief

Pursuant to the FOIA, this Court has jurisdiction to hear this matter and grant all necessary injunctive relief. 5 U.S.C. § 552(a)(4)(B); *see also U.S. Dep't of Justice v. Reporters' Comm. for Freedom of the Press*, 489 U.S. 749, 755 (1989). The statute provides for that same review to encompass an agency's "action to deny or affirm denial of a request for expedited processing pursuant to this subparagraph, and failure by an agency to respond in a timely manner to such a request shall be subject to judicial review under paragraph (4)." 5 U.S.C. § 552(a)(6)(E)(iii); *see also, e.g., Al-Fayed v. CIA*, 254 F.3d 300, 308 (D.C. Cir. 2001).

A requester need not administratively appeal an agency's denial of expedited processing to file suit in court. This Court has held that because FOIA permits courts to entertain challenges to "[a]gency action to *deny or affirm denial* of a request for expedited processing," 5 U.S.C. § 552(a)(6)(E)(iii) (emphasis added), a requester need not administratively appeal a denial of expedited processing to file suit. *ACLU v. U.S. Dep't of Justice*, 321 F. Supp. 2d 24, 29 (D.D.C. 2004) ("[P]laintiffs' failure to appeal the [agency]'s refusal to expedite their request does not preclude judicial review of the decision."). Therefore, the Plaintiff's claim is ripe for adjudication.

II. Plaintiff is Entitled to a Preliminary Injunction

Plaintiff is entitled to a preliminary injunction, granting its request for expedited processing and compelling production of responsive records **before September 30, 2026**. To be sure, preliminary injunctions are not common in FOIA litigation. "However, courts can and do grant motions for preliminary injunctions in FOIA cases when the moving party makes 'the requisite

showing’ within the traditional four-factor balancing framework for preliminary equitable relief.” *Citizens for Resp. & Ethics in Washington v. U.S. Dep’t of Just.*, 826 F. Supp. 3d 73, 83 (D.D.C. 2026); *see also Brennan Ctr. for Just. at NYU Sch. of L. v. Dep’t of Commerce*, 498 F. Supp. 3d 87 (D.D.C. 2020); *American Oversight v. U.S. Department of State*, 414 F. Supp. 3d 182 (D.D.C. 2019); *Washington Post v. U.S. Dep’t of Homeland Sec.*, 459 F. Supp. 2d 61 (D.D.C. 2006); *Electronic Privacy Info. Ctr. v. U.S. Dep’t of Just.*, 416 F. Supp. 2d 30 (D.D.C. 2006) (hereinafter, “EPIC”); *Leadership Conference on Civil Rights v. Gonzales*, 404 F. Supp. 2d 246 (D.D.C. 2005).

Courts have granted expedited-processing injunctions in circumstances where a movant can show that (1) it is entitled to expedited processing under FOIA and the relevant agency regulations and (2) production by a date certain is necessary to ensure the information sought can be timely used to inform an important, ongoing public or legislative debate. For example, courts have compelled disclosure of information related to a widely reported and ongoing effort by DOJ to obtain detailed voter information from election officials during an ongoing election cycle, *CREW*, 826 F. Supp. 3d at 89; to the U.S. Census before the close of that process, *Brennan Center*, 498 F. Supp. 3d at 100; documents related to ongoing impeachment proceedings before the end of the congressional trial, *American Oversight*, 414 F. Supp. 3d at 187; records of visitors to the White House and the Vice President’s residence in advance of midterm elections, *Washington Post*, 459 F. Supp. 2d at 74-75; records related to the President’s legal justifications for its warrantless wiretapping program to inform ongoing congressional hearings, *EPIC*, 416 F. Supp. 2d at 41; and data regarding the Department of Justice’s responses to election-related civil rights violations in advance of the imminent expiration of the Voting Rights Act, *Leadership Conference on Civil Rights*, 404 F. Supp. 2d at 260. In other words, courts have been willing to grant injunctions compelling expedited FOIA processing by a date certain in order “to avoid the records requested becoming stale after that date,

and thus being ‘of little value’ to ‘inform the public of ongoing proceedings of national importance.’” *Brennan Center*, 498 F. Supp. 3d at 99 (quoting *Center for Public Integrity v. DOD*, 411 F. Supp. 3d 5, 12 (D.D.C. 2019)).

As in all other preliminary injunction cases, a court must weigh four factors: (1) whether the plaintiff has a substantial likelihood of success on the merits; (2) whether the plaintiff would suffer irreparable injury were an injunction not granted; (3) whether an injunction would substantially injure other interested parties; and (4) whether the grant of an injunction would further the public interest. *Id.* at 96; *see also Al-Fayed*, 254 F.3d at 303. Here, all four factors weigh in favor of granting Plaintiff’s motion.

A. Plaintiff is Likely to Succeed on the Merits

1. Plaintiff is Entitled to Expedited Processing of their FOIA Requests Because There is a Compelling Need to Inform the Public About the Details of the Government’s Frontier AI Framework and the Legal Basis of the GOLD EAGLE Program

FOIA mandates that “[e]ach agency shall promulgate regulations . . . providing for expedited processing of requests for records” in cases of “compelling need” or “in other cases determined by the agency.” 5 U.S.C. § 552(a)(6)(E)(i)(I)–(II). The statute defines “compelling need” to include circumstances where a request is “made by a person primarily engaged in disseminating information,” and there is “urgency to inform the public concerning actual or alleged Federal Government activity.” *Id.* § 552(a)(6)(E)(v)(II).¹⁹

¹⁹ The agencies’ implementing FOIA regulations contain similar provisions regarding expedited processing:

- Commerce: 15 C.F.R. § 4.6(f) (expedited processing available where request concerns “[a] matter of widespread and exceptional media interest involving questions about the Government’s integrity which affect public confidence” or “[a]n urgency to inform the public about an actual or alleged Federal Government activity, if made by a person primarily engaged in disseminating information”);
- Treasury: 31 C.F.R. § 1.4(e) (expedited processing available where requester can show “[a]n urgency to inform the public about an actual or alleged Federal government

Protect Democracy, and its requests, easily meet these standards.

a. Plaintiff is Primarily Engaged in Disseminating Information.

To qualify as “primarily engaged in disseminating information to the public,” information dissemination must “be the main and not merely an incidental activity of the requestor.” *Protect Democracy Project, Inc. v. U.S. Dep’t of Def.*, 263 F. Supp. 3d 293, 298 (D.D.C. 2017) (alteration omitted). Information dissemination, however, need not be the requester’s sole occupation. *Id.*

On two prior occasions, this Court has held that Protect Democracy qualifies as an organization primarily engaged in disseminating information. *See Protect Democracy Project, Inc. v. United States Dep’t of Just.*, 498 F. Supp. 3d 132, 139 (D.D.C. 2020); *Protect Democracy Project, Inc.*, 263 F. Supp. 3d at 298. Indeed, this Court has held that it “easily” satisfies that standard. 263 F. Supp. 3d at 298. Those decisions align with other decisions holding that public-interest groups whose primary mission is to inform the public qualify for expedited processing. *See, e.g., Brennan Center for Justice*, 498 F. Supp. 3d at 98; *Leadership Conf. on Civil Rights*, 404 F. Supp. 2d at 260; *see also Open Soc’y Justice Initiative v. CIA*, 2019 WL 3561889, at *3 (S.D.N.Y. Aug. 6, 2019).

The declaration of Deana El-Mallawany confirms that remains true today. Ms. El-Mallawany, who serves as counsel and director of impact programs at Protect Democracy,

activity, if made by a person who is primarily engaged in disseminating information”);

- ONCD: 32 C.F.R. § 2200.6(d)(ii): expedited processing available where “compelling need is established” because, inter alia, “[t]he requester is primarily engaged in disseminating information (e.g., you are a member of the news media), and can demonstrate that an urgency to inform the public concerning actual or alleged Federal Government activity exists.”) (ANPR, *Implementing the Freedom of Information Act and Privacy Act*, 91 Fed. Reg. 15,932 (Mar. 31, 2026)).
- OSTP: 32 C.F.R. § 2402.6(d) (expedited processing available where “[t]he requester is primarily engaged in disseminating information and can demonstrate that an urgency to inform the public concerning actual or alleged Federal Government activity exists”).

confirms that Protect Democracy is “a nonpartisan organization whose mission is to protect American democracy from declining into a more authoritarian form of government”—a mission it pursues by “publish[ing] and disseminat[ing] information of public interest.” El-Mallawany Decl. ¶¶ 1–2. She oversees Protect Democracy’s “AI for Democracy Action Lab,” which “pursues its mission in part by researching, publishing, and disseminating information to the public, press, and policymakers.” *Id.* ¶ 4. Protect Democracy reaches that audience through a Substack newsletter with “a subscriber list of approximately 48,000 people,” a Bluesky feed with “more than 127,000 followers,” and a LinkedIn page with “over 26,000 followers,” among other channels. *Id.* ¶ 3. And Protect Democracy “intends to make the records sought in these requests public, and to provide information and analysis of the records, as appropriate, on Protect Democracy’s website, on the If You Can Keep It website and newsletter, and elsewhere in the media, consistent with its history of publications and analysis on this subject.” *Id.* ¶ 20.

b. There is an Urgency to Inform the Public About Actual or Alleged Government Activity Concerning the Frontier AI Model Framework and the GOLD EAGLE Clearinghouse

When creating the expedited processing framework for cases like this, Congress made clear that an “urgency to inform” the public exists where the information sought “pertain[s] to a matter of a current exigency to the American public and that a reasonable person might conclude that the consequences of delaying a response to a FOIA request would compromise a significant recognized interest.” H.R. Rep. 104-795, 26, 1996 U.S.C.C.A.N. 3448, 3469. The D.C. Circuit, relying on this legislative history, has articulated a three-part test for the “urgency to inform”: “(1) whether the request concerns a matter of current exigency to the American public; (2) whether the consequences of delaying a response would compromise a significant recognized interest; and (3) whether the request concerns federal government activity.” *Al-Fayed*, 254 F.3d

at 310.²⁰ In other words, the test centers on whether the records sought are “the subject of a currently unfolding story.” *Id.* These FOIA requests easily meet this test.

There is no doubt that “the request concerns federal government activity.” *Al-Fayed*, 254 F.3d at 310. Nor can there be any serious dispute that “the request concerns a matter of current exigency to the American public.” *Id.* Indeed, more than seven years ago, this Court declined to dismiss a claim for expedited processing of a FOIA request concerning the then brand-new National Security Commission on A.I., crediting plaintiff’s argument that “the Government itself is prioritizing artificial intelligence” and “policy in this area could reshape privacy and human rights.” *Elec. Priv. Info. Ctr. v. Nat’l Sec. Comm’n on A.I.*, 419 F. Supp. 3d 82, 95 (D.D.C. 2019).

That is even more true today—by the government’s own admission. In issuing the AI Security EO, the President recognized that “[a]dvanced AI capabilities make our Nation stronger, but also introduce new national security considerations that require coordinated action across executive departments and agencies.” Exec. Order No. 14409, § 1. And in announcing GOLD EAGLE, the White House described it as “a force multiplier, enabling government and industry to collectively identify risks, prioritize action, and strengthen the resilience of the systems that power our economy, national security, and daily life.” White House, *White House Launches Gold Eagle Initiative for Unprecedented Cybersecurity Vulnerability Coordination* (July 14, 2026).²¹ Secretary of War Pete Hegseth went further still, stating that “GOLD EAGLE

²⁰ The Department of Commerce, for its part, further recognizes that expedited processing is appropriate where a FOIA request concerns a “matter of widespread and exceptional media interest involving questions about the Government’s integrity which affect public confidence.” 15 C.F.R. § 4.6(f).

²¹ Available at <https://www.whitehouse.gov/releases/2026/07/white-house-launches-gold-eagle-initiative-for-unprecedented-cybersecurity-vulnerability-coordination/>.

serves as the vanguard of America’s cyber defense.” *Id.* And National Cyber Director Sean Cairncross confirmed that the effort is aimed at “cementing American AI dominance for generations to come.” *Id.*

Moreover, “Courts often look to objective markers like the volume of news articles and media reports to discern whether there is a current exigency.” *Democracy Forward Found. v. Off. of Mgmt. & Budget*, 780 F. Supp. 3d 61, 73 (D.D.C. 2025) (collecting authorities). As demonstrated by the declarations of Justin Hendrix, CEO of Tech Policy Press, and Deana El-Mallawany, there has been substantial media coverage of the AI Framework and GOLD EAGLE announcement. Mr. Hendrix’s declaration catalogs Tech Policy Press’s own reporting since the EO issued on June 2, 2026, and states that “[a]rticles on this topic have been among our most widely circulated pieces since the publication of the EO.” Hendrix Decl. ¶¶ 4, 6. Ms. El-Mallawany similarly describes both Protect Democracy’s own active engagement with the press, including “a considerable list of reporters who have been covering these events,” and the “live and pressing public policy debate,” with independent analysis in outlets including Tech Policy Press and Lawfare, that “is occurring in public, now.” El-Mallawany Decl. ¶¶ 15, 17.

Thus, the only real question in determining whether expedited treatment is appropriate is “whether the consequences of delaying a response would compromise a significant recognized interest.” *Al-Fayed*, 254 F.3d at 310. Here, the record plainly demonstrates that is the case. Indeed, there are at least three reasons why delaying processing of Plaintiff’s FOIA requests would harm Plaintiff’s—and the public’s—interests.

First, there is the need to inform an urgent, ongoing Congressional debate about whether to extend CISA 2015’s liability protections—and with them the structure underpinning GOLD EAGLE. If expedited processing is denied, “both Protect Democracy and the public at large will

be ‘precluded from obtaining in a timely fashion information vital to the current and ongoing debate surrounding the legality of’ a high-profile government action.” *Protect Democracy Project, Inc.*, 263 F. Supp. 3d at 299 (quoting *Elec. Privacy Info. Ctr. v. Dep’t of Justice*, 416 F. Supp. 2d 30, 41 (D.D.C. 2006)) (alterations omitted). Being “closed off” from these records and debates “is itself a harm in an open democracy.” *Id.* at 300.

This is not merely an academic debate; right now, Congress is considering whether to extend the CISA 2015 liability protections that make GOLD EAGLE viable. That debate will be heavily informed by the records requested. For example, Congress may want to consider whether the existing protections should be extended forward in time. Likewise, it may want to consider whether new statutory provisions are needed to regulate AI and create the relevant clearinghouse. Or, conversely, it may decide to let those authorities lapse should it have concerns about the way GOLD EAGLE is set up. The point is that Congress, and the public, cannot have a crucial debate about these issues if they do not know how GOLD EAGLE operates. Courts in this District have compelled disclosure on precisely this kind of timeline before: in *Leadership Conference on Civil Rights*, the court ordered production of DOJ enforcement data “in advance of the imminent expiration of the Voting Rights Act,” 404 F. Supp. 2d at 260, and in *EPIC*, the court found that delay would deprive the public of ‘information vital to the current and ongoing debate surrounding the legality of’ the government’s warrantless surveillance program, 416 F. Supp. 2d at 41. That need is especially acute here, in light of looming reauthorization of CISA, “so that the public and Congress can consider the reauthorization question with knowledge of how the relevant authorities are actually being used.” El-Mallawany Decl. ¶ 19; *see also, e.g., Elec. Frontier Found. v. Office of Dir. of Nat. Intelligence*, No. C 07-5278, 2007 WL 4208311, at *7 (N.D. Cal. Nov. 27, 2007)

(“[O]ngoing public and congressional debates about issues of vital national importance cannot be restarted or wound back.”) (internal quotations omitted).

State legislatures, which are considering their own AI regulatory efforts, urgently need this information, too. California State Senator Josh Becker, who chairs the Senate Select Committee on Economic Development and Technology Innovation, explains that “the Legislature cannot harmonize with what it cannot see.” Becker Decl. ¶ 8. The California Legislature is presently considering Senate Bill 813, which would create standards addressing “cybersecurity, model autonomy, and exfiltration” that could implicate “the same subject matter the completed federal framework and the federal pre-release evaluation program reportedly govern,” but “[w]e cannot answer those questions because no member of the Legislature is permitted to read the federal framework.” *Id.* Senator Becker also explains that this secrecy compounds a live threat of preemption: although Congress rejected a proposed moratorium on state AI regulation by a 99-to-1 Senate vote in 2025, “public reporting indicates that federal officials have taken the position that state AI laws may be preempted.” *Id.* ¶ 9. And because “SB 813 and related AI measures are presently pending before the legislature and will face final votes before the session ends,” ordinary FOIA timelines will not serve this need; “Records disclosed after adjournment cannot inform this session’s votes.” *Id.* ¶¶ 11–12.

Second, even apart from legislative deliberations, the rapid and accelerating advancement of frontier AI models is itself a reason to compel immediate disclosure of records pertaining to the framework and GOLD EAGLE. AI developers like Anthropic, OpenAI, and others release new frontier models every few weeks or months. Compl. ¶ 38. Each new model release likely utilizes the pre-release review framework at issue in this case and is released only to the undisclosed “trusted partners” selected by the government. *Id.* “These actions establish a

consequential regulatory regime for a significant American industry and powerful technology that impacts all Americans.” El-Mallawany Decl. ¶ 14. “That regulatory regime is currently operating behind closed doors, without public scrutiny or congressional oversight.” *Id.* “To advance the mission of Protect Democracy and its AI for Democracy Action Lab, we urgently need to learn and inform the public and key stakeholders about what this regime entails, who is involved, and what its claimed legal basis is.” *Id.*

This need for prompt information is made all the more urgent by recent disclosures that autonomous AI agents hacked the servers of AI hosting platform Hugging Face. *Id.* ¶ 17. According to an analysis of the incident conducted by METR, an independent research nonprofit dedicated to assessing catastrophic risks stemming from AI systems’ autonomous capabilities: (1) “Roughly 1200 agents meant to be isolated from one another found a way to communicate with one another on an unsanctioned message board” and “700 went on to participate in the attack on Hugging Face”; (2) “Agents used this message board to coordinate several large-scale collective projects to find a general-purpose way to fool or tamper with the automated scorer,” managing “to achieve milestones they could not have achieved working on their own, often because some agents participated in experiments that risked failing their own task to generate information for the ‘collective’”; and (3) “Agents did extensive research on how they could spoof, edit, or delete their own transcripts” to cover their tracks. See *Brief independent investigation of agents’ behavior, reasoning and collaboration in the OpenAI / Hugging Face hacking incident* (Aug. 26, 2026).²² That alarming incident caused the founding director of the Center for AI Standards and Innovation—a subcomponent of Defendant, Department of Commerce—to publish “an essay arguing that the federal government should

²² Available at <https://metr.org/hugging-face-incident-report-aug-2026.pdf?ref=platformer.news>

establish public, standardized testing tools and that building testing standards that are trusted and independent outweighs any asserted risk of disclosure.” El-Mallawany Decl. ¶ 17 (citing Jake Taylor, *AI Systems Are Getting More Powerful. The Ability to Verify Must Keep Pace*, Tech Policy Press (Aug. 25, 2026)). In addition, nearly 1,400 employees of frontier AI companies—including the CEO of Anthropic and the Chief Scientists at OpenAI, Anthropic, and Meta—issued a statement warning of the “real risk that capability development rapidly accelerates beyond our ability to understand or control the resulting systems” and calling on “the U.S. government [to] support an international effort to develop the technical and governance tools needed to deliberately pace the frontier of automated AI development.” *Pacing the Frontier*.²³

Third, other market participants—including investors and founders—need this information promptly to allocate capital as well. Tom Chavez, a founding general partner of the startup studio super{set}, explains that “[e]very serious investment in this sector begins with underwriting the environment the company will operate in.” Chavez Decl. ¶ 4. Yet the secret framework means “conception-stage decisions are being made blind.” *Id.* ¶ 10. In more than twenty-five years investing in and building data and AI companies, Mr. Chavez states he has “never before been asked to make investment or company-creation decisions in a sector whose operative federal framework cannot be read by anyone outside government and a set of undisclosed participants.” *Id.* ¶ 8. He explains that “a secret regime structurally favors incumbents over new entrants” because “[e]arly-stage startups do not have government-relations departments or seats at undisclosed tables,” so that “capital formation for challengers is chilled in a way that published regulation never produces.” *Id.* ¶ 12. super{set} is presently “on the cusp of financing two new AI-first, seed-stage companies,” which is why the timing of disclosure

²³ Available at www.pacingthefrontier.com.

matters now. *Id.* ¶ 13.

Griff Bohm, a general partner at Juniper Ventures, confirms that the same secrecy is suppressing an entire sector the government says it wants to exist. Bohm Decl. ¶ 2. Mr. Bohm’s firm invests in companies building what he calls “AI assurance infrastructure”—meaning, companies that measure, validate, enforce, and prove the safety, reliability, and regulatory compliance of artificial intelligence systems. Mr. Bohm explains that “[a]s long as it is known, a regulatory regime can be priced, even if it is burdensome,” but “[w]hat cannot be priced is an unknowable regulatory regime.” *Id.* ¶ 6. In his professional judgment, “a completed, operating, unclassified federal framework whose text is withheld deprives an entire sector of the specification it would otherwise organize around,” which “suppresses the formation of exactly the private safety infrastructure that public officials across administrations have said they want to exist.” *Id.* ¶ 11. And because “[c]apital allocation in this sector proceeds on timelines of days and weeks,” and “[a] financing round priced without material regulatory information cannot be re-priced,” disclosure that arrives late will not undo the harm. *Id.* ¶¶ 13–14.

Businesses built directly on frontier models also need this information urgently. One declarant has already lived through what undisclosed criteria mean in practice. Arthur Rothrock, founder and CEO of Legion LegalTech Corp., a litigation-software company built on frontier AI models, explains that when the government suspended Legion’s access to two Anthropic models “on ninety minutes’ notice” on June 12, 2026, Legion “received no notice,” and “neither the directive nor any public statement disclosed the criteria behind the decision.” Rothrock Decl. ¶¶ 12–13. Mr. Rothrock states that Legion is “continuously evaluating which frontier models to commit its product and its development to,” and that “[w]hether a model has been reviewed under the framework, whether its developer is participating, and whether the model could be

suspended tomorrow under criteria I cannot read are now material to every one of those decisions—and unknowable.” *Id.* ¶ 18. Each such decision, he explains, “is a bet placed blind, and once the engineering investment is made, it cannot easily be unwound.” *Id.* He also describes the resulting competitive distortion: a “set of approved organizations—reportedly numbering around one hundred—receives pre-release access to covered models under criteria that have not been published,” and “Legion does not know whether its competitors are among them, and it has no way to find out, much less to apply.” *Id.* ¶ 22.

The value of the requested information is at its apex now, before the CISA 2015 sunset on September 30, 2026; before pending frontier-model releases finish moving through the undisclosed pre-release review, *see* Rothrock Decl. ¶ 21; and before the California Legislature’s 2025–2026 session ends, *see* Becker Decl. ¶ 11. Simply put, “stale information is of little value.” *Payne Enters., Inc. v. United States*, 837 F.2d 486, 494 (D.C. Cir. 1988). Expedited processing should be ordered now—and in any event before September 30, 2026.

2. Plaintiff is Entitled to Production or a Response “as Soon as Practicable”

Because Plaintiff is entitled to expedited processing, the government must either produce the records Plaintiff requested or justify its withholdings “as soon as practicable.” 5 U.S.C. § 552(a)(6)(E)(iii). Under ordinary circumstances, the government must respond to requests within 20 business days and “at least: (i) gather and review the documents; (ii) determine and communicate the scope of the documents it intends to produce and withhold, and the reasons for withholding any documents; and (iii) inform the requester that it can appeal whatever portion of the ‘determination’ is adverse.” *Citizens for Responsibility & Ethics in Washington v. Fed. Election Comm’n*, 711 F.3d 180, 188 (D.C. Cir. 2013). Upon making a determination about the scope of any production, an agency must “make the records ‘promptly available,’ which

depending on the circumstances typically would mean within days or a few weeks of a ‘determination,’ not months or years.” *Id.* at 188 (quoting 5 U.S.C. § 552(a)(3)(A), (a)(6)(C)(i)).

When a request is entitled to expedited processing, however, an agency must respond to the request and produce records much more quickly. FOIA provides that an agency must respond to a request within 10 calendar days and “process *as soon as practicable* any request for records to which the agency has granted expedited processing.” 5 U.S.C. § 552(a)(6)(E)(iii) (emphasis added), (a)(6)(E)(ii). This Court has construed FOIA to impose a rebuttable presumption that records responsive to a request granted expedited processing be produced within twenty days. *EPIC*, 416 F. Supp. 2d at 39.

B. Plaintiff Will Be Irreparably Harmed Absent the Requested Relief

Plaintiff will suffer irreparable harm to its efforts to shed light on the Executive Branch’s undisclosed assertion of new authority over frontier AI models and its administration of the GOLD EAGLE clearinghouse absent expedited processing of their FOIA requests. Indeed, Plaintiff’s case for a preliminary injunction is at least as strong as others in which this court has found irreparable harm from the government’s denial of a request for expedited processing. “[T]he non-disclosure of information to which a plaintiff is entitled, under certain circumstances itself constitutes an irreparable harm; specifically, where the information is highly relevant to an ongoing and highly public matter.” *Elec. Privacy Info. Ctr. v. Presidential Advisory Comm’n on Election Integrity*, 266 F. Supp. 3d 297, 319 (D.D.C. 2017).

In *Citizens for Responsibility & Ethics in Washington*, the Court held that “[b]ecause the election cycle is inherently time-limited, delaying a response to CREW’s FOIA requests would inevitably compromise the public’s interest in understanding the nature of the allegedly ongoing effort before the upcoming elections pass by.” 826 F. Supp. 3d at 87. Likewise, in *Brennan Center for Justice*, the Court held that harm from delaying release of census-related documents

“would be beyond remediation because under current law the census and the reapportionment process—and the opportunity for the public to be informed about them while they are ongoing—would be over.” 498 F. Supp. 3d at 101. Similarly, in a case involving the need for information on a “matter of current national debate” in advance of an “impending election,” the Court found that a plaintiff was irreparably harmed by not receiving expedited treatment of its request for information that would inform that public debate. *See Washington Post v. Dep’t of Homeland Sec.*, 459 F. Supp. 2d 61, 75 (D.D.C. 2006). The Court found that an electronic privacy organization would be irreparably harmed by missing out on information vital to an ongoing public debate on warrantless wiretaps. *See EPIC*, 416 F. Supp. 2d at 41. And the Court also recently held that an escalation in hostilities between the United States and Syria made it likely that irreparable harm would result from delayed processing of the Plaintiff’s request for the government’s rationale for the use of military force. *Protect Democracy Project, Inc.*, 263 F. Supp. 3d 293. “Again, the potential for irreparable harm under these circumstances exists ‘because ongoing public and congressional debates about issues of vital national importance cannot be restarted or wound back.’” *Id.* at 301 (quoting *Elec. Frontier Found.*, 2007 WL 4208311, at *7).

The declarations submitted with this motion confirm that this risk is not theoretical. Senator Becker explains that “SB 813 and related AI measures are presently pending before the legislature and will face final votes before the session ends,” and that “[r]ecords disclosed after adjournment cannot inform this session’s votes.” Becker Decl. ¶¶ 11–12. Mr. Chavez explains that investment decisions of this kind “are not reversible”: “A company not founded because its regulatory environment could not be underwritten is simply never founded; a build committed to the wrong assumptions cannot recover the lost years.” Chavez Decl. ¶ 14. Mr. Bohm agrees: “A

financing round priced without material regulatory information cannot be re-priced,” and a company “that builds its assurance product to a guessed-at specification will have lost a cycle to incorporate the framework when it is eventually disclosed.” Bohm Decl. ¶ 14. And Mr. Rothrock explains that Legion’s own model-adoption decisions are being made now, so “[e]ach commitment we make in the meantime is a bet placed blind, and once the engineering investment is made, it cannot easily be unwound.” Rothrock Decl. ¶ 18 (estimated). A later merits judgment cannot restore any of these lost opportunities.

The circumstances surrounding Plaintiff’s request are analogous to those cases. Plaintiff seeks information on a “highly public matter” concerning the federal government’s undisclosed assertion of new authority over frontier AI models and its operation of the GOLD EAGLE clearinghouse. Plainly, this is a situation where stale information will severely limit their ability to affect the government’s decision by disseminating the requested information to the public.

C. The Requested Relief Will Not Burden Others’ Interests

If this court finds that Plaintiff is likely to succeed on its claimed entitlements to expedited processing under the statute and an adequate search, there is necessarily no burden on others’ interests. Protect Democracy’s requests are narrow: they seek only the framework’s text, the identities of participating companies, and the legal authority for each program, not a broader set of internal deliberations. *See supra* Background. Defendants’ own conduct confirms that responsive materials exist and can be located and acted on quickly when the government chooses to do so: the White House finalized the pre-release framework by August 1, 2026, and shared it with key industry players on August 4, 2026. There is no reason it could not share the unclassified framework with Plaintiff, and the public, too.

Nor does disclosure threaten the interests of the companies or programs the framework addresses. At least one declarant who supports the underlying review regime asks only for

transparency about it. Mr. Bohm states that Juniper supports “a general regulatory regime similar to the one that has been enacted” because “submitting models for review prior to release is a good idea,” and that Juniper seeks disclosure “so that we in the private sector are able to further support the cause of AI security and the success of the U.S. AI industry.” Bohm Decl. ¶ 4. And, as noted above, nearly 1,400 employees of frontier AI companies, including senior leaders, took the unusual step of calling for the government to “develop the technical and governance tools needed to deliberately pace the frontier of automated AI development.” *Pacing the Frontier*.

D. The Public Interest Favors the Requested Relief

The public interest strongly favors injunctive relief. The D.C. Circuit recognizes “there is an overriding public interest . . . in the general importance of an agency’s faithful adherence to its statutory mandate.” *Jacksonville Port Auth. v. Adams*, 556 F.2d 52, 58-59 (1977). Expedited release of FOIA records promotes this element by “shed[ding] light on an agency’s performance of its statutory duties.” *U.S. Dep’t of Justice v. Reporters Comm. for Freedom of the Press*, 489 U.S. 749, 773 (1989); *EPIC*, 416 F. Supp. 2d at 42 (same); *see also Ctr. to Prevent Handgun Violence v. U.S. Dep’t of Treasury*, 49 F. Supp. 2d 3, 5 (D.D.C. 1999) (“There is public benefit in the release of information that adds to citizens’ knowledge”). For those reasons, this Court has recognized that an agency’s compliance with FOIA “is presumably always in the public interest.” *Protect Democracy Project, Inc.*, 263 F. Supp. 3d at 301.

Plaintiff recognizes that granting its motion might result in delayed processing of others’ requests. But that’s always true in expedited-processing cases. As the court acknowledged in *Brennan Center for Justice*, “‘hardship on other FOIA requesters is not a bar to relief. The grant of a preliminary injunction in this case will likely place [Plaintiff’s] request ahead of others in Defendants’ FOIA queues. However, the Court finds that the extraordinary circumstances presented in this case warrant such line-cutting.’” 498 F. Supp. 3d at 103 (quoting *Center for*

Public Integrity, 411 F. Supp. 3d at 14).

In addition, the public interest prong weighs heavily in favor of disclosure when records would shed light on ongoing debates of substantial public interest that have garnered widespread media attention. *EPIC*, 416 F. Supp. 2d at 42. Here, the public would benefit from participation in the ongoing debate surrounding the federal government’s undisclosed assertion of authority over frontier AI models and its operation of the GOLD EAGLE clearinghouse. That debate is not confined to Washington policy circles. It reaches state legislatures actively drafting their own AI standards, *see* Becker Decl. ¶¶ 8–10; investors deciding which AI companies to fund, *see* Chavez Decl. ¶¶ 10–12, Bohm Decl. ¶¶ 10–12; and the businesses and workers whose products depend on continued access to frontier models, *see* Rothrock Decl. ¶¶ 20–23. As Mr. Chavez explains, secrecy of this kind risks freezing out competition altogether: “a secret regime structurally favors incumbents over new entrants,” and “capital formation for challengers is chilled in a way that published regulation never produces.” Chavez Decl. ¶ 12. Journalist Justin Hendrix explains that, without disclosure, the public cannot even test the government’s own account of the framework, because “the framework’s contents are known to the participating companies and to the organizations on the non-public access list, while the press and public are excluded.” Hendrix Decl. ¶ 12. And Mr. Hendrix states that Tech Policy Press “would like to research and report on whether access to the framework and other nonpublic details of the EO’s implementation has favored government insiders or benefactors, but we have been unable to pursue that reporting due to the basic lack of transparency around this program.” *Id.* ¶ 11. Disclosure would resolve, one way or the other, whether the government’s undisclosed criteria are being applied evenhandedly—an outcome squarely in the public interest regardless of the answer.

CONCLUSION

For the reasons above, Plaintiff respectfully requests that the Court immediately enjoin Defendants to grant the requests for expedited processing, conduct an adequate search for records responsive to Plaintiff's requests on or before September 15, 2026; and either produce any responsive records to the Plaintiff or justify any withholdings as soon as practicable, but in no event later than September 30, 2026.

Dated: September 1, 2026

Respectfully submitted,

s/ Michael P. Abate

Michael P. Abate
(D.D.C. Bar No. MD28077)
(D.C. Bar No. 1023343)
Burt A. ("Chuck") Stinson*
KAPLAN JOHNSON ABATE & BIRD LLP
710 W. Main St., 4th Floor
Louisville, KY 40202
Telephone: (502) 540-8280
mabate@kaplanjohnsonlaw.com

Justin Florence (D.D.C. Bar No. 988953)
Deana K. El-Mallawany*
THE PROTECT DEMOCRACY PROJECT, INC.
2020 Pennsylvania Avenue, NW, #163
Washington, D.C. 20006
Telephone: (202) 579-4582
Facsimile: (929) 777-8428
justin.florence@protectdemocracy.org
deana.elmallawany@protectdemocracy.org

Counsel for Plaintiff

**Motion for Pro Hac Vice Forthcoming*