UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

THE PROTECT DEMOCRACY PROJECT, INC.
2020 Pennsylvania Ave., NW #163
Washington, DC 20006,

Plaintiff,

v.

OFFICE OF THE NATIONAL CYBER DIRECTOR
725 17th St., NW
Washington, DC 20006,

OFFICE OF SCIENCE AND TECHNOLOGY POLICY
Eisenhower Executive Office Building
1650 Pennsylvania Ave., NW
Washington, DC 20504,

U.S. DEPARTMENT OF COMMERCE, BUREAU OF INDUSTRY AND SECURITY
1401 Constitution Ave., NW, Room 6622
Washington, DC 20230, and

U.S. DEPARTMENT OF THE TREASURY,
1500 Pennsylvania Ave., NW
Washington, DC 20220,

Defendants.

Case No. _____

COMPLAINT

Plaintiff Protect Democracy Project, Inc. ("Protect Democracy"), by its undersigned attorneys, alleges:

INTRODUCTION

1. This is an action under the Freedom of Information Act (FOIA), 5 U.S.C. § 552, to compel expedited disclosure of the rules by which the federal government now governs the most consequential technology of this era. Since June 2026, the Executive Branch has built a

regime of extraordinary power over frontier artificial intelligence (AI) models, deciding which models may be released, when, and to whom. And it has done so almost entirely in secret.

2. Neither the public nor Congress has seen the rules of the governance regime, but its force and significance are clear. In June, the Department of Commerce gave a leading developer ninety minutes to comply with a directive resulting in the suspension of worldwide access to its most advanced models. In July, four agencies launched a standing government-industry coordination body called GOLD EAGLE with nothing visible to the public but a short press release. And on August 3, the White House announced that it had completed a framework for reviewing AI models before their public release, but declined to disclose what the framework contains, who has agreed to it, or the legal basis for it, even while acknowledging that the framework is not classified. As one White House official reportedly put it, "Just because things are unclassified that doesn't mean we are going to broadcast them to everyone."

3. But the government has revealed this regime to a select few. The framework and the terms of these programs have been shared with a select set of AI companies, exacerbating the already severe information asymmetry between a small group of industry insiders and everybody else who can only hope this powerful technology is being governed safely and in the public interest.

4. As a result of all of this, there now exists a secret de facto regulatory regime governing the most consequential technology in the world. This technology, these companies, and this framework impact nearly every major aspect of American society, from national security to the economy to American's individual liberties, and the entire framework has been drafted and is being applied in secret, pursuant to unknown legal authorities. This is happening at a moment when two of the leading companies are reportedly preparing for public offerings that are

expected to be among the largest in history, with ramifications for the national and global economy, and at a time when AI safety groups and some of the companies themselves are warning of potentially society-destabilizing risks from these technologies.

5. On August 7, 2026, Protect Democracy submitted FOIA requests to the four Defendant agencies seeking the framework's text, the participants in and legal authority for these programs, and the terms of participation, and requesting expedited processing because the value of these records is measured in weeks. Congress must decide as soon as September 30, absent extension, whether to reauthorize the statutory protections the government says GOLD EAGLE requires, and new frontier models are moving through the secret review process now, while the public learns of alarming behavior by AI agents in emerging models. Given the agencies' lack of response or production of documents, Protect Democracy brings this suit and seeks an injunction to enforce its expedited processing request so that it may disseminate the produced documents in time to inform the imminent decisions numerous actors across society need to make regarding these companies, technologies, and regulatory questions.

JURISDICTION AND VENUE

6. This Court has jurisdiction over this FOIA action pursuant to 28 U.S.C. § 1331 and 5 U.S.C. § 552(a)(4)(B).

7. Venue is proper pursuant to 5 U.S.C. § 552(a)(4)(B).

PARTIES

8. Plaintiff Protect Democracy is a non-partisan, non-profit section 501(c)(3) organization whose mission is to prevent American democracy from declining into a more authoritarian form of government. Protect Democracy engages in public education about threats to democratic norms and institutions and how the American people can best confront them. It advances its mission through research, analysis, technology, and litigation to stand up for free

and fair elections, the rule of law, fact-based debate, and a better democracy for future generations. As part of this mission, Plaintiff seeks to inform public understanding of operations and activities of the government by gathering and disseminating information that is likely to contribute significantly to the public understanding of Executive Branch operations and activities. Plaintiff regularly requests such information pursuant to FOIA. The organization is incorporated under the laws of the District of Columbia.

9. Defendant Office of the National Cyber Director (ONCD) is an office within the Executive Office of the President that coordinates and implements national cyber policy and strategy in the Executive Branch. It is an "agency" under 5 U.S.C. § 551(1) and is therefore subject to FOIA. *See* ONCD, Implementing the Freedom of Information Act and Privacy Act, 91 Fed. Reg. 15,932 (March 31, 2026) (proposed ONCD FOIA regulations); *see also* 6 U.S.C. § 1500 (creating ONCD).

10. Defendant Office of Science and Technology Policy (OSTP) is an office within the Executive Office of the President that coordinates the nation's science and technology policy. It is an "agency" under 5 U.S.C. § 551(1) and is therefore subject to FOIA. *See* 32 C.F.R. Part 2402 (OSTP FOIA regulations); *see also* 42 U.S.C. § 6611 (creating OSTP).

11. Defendant U.S. Department of Commerce, Bureau of Industry and Security (BIS) is a Federal agency that, *inter alia*, administers certain export control and treaty compliance rules. It is an "agency" under 5 U.S.C. § 551(1) and is therefore subject to FOIA. *See* 15 C.F.R. Part 4 (Department of Commerce FOIA regulations applicable to BIS).

12. Defendant U.S. Department of the Treasury ("Treasury") is a Federal cabinet agency responsible for a range of economic and financial missions. It is an "agency" under 5

U.S.C. § 551(1) and is therefore subject to FOIA. *See* 31 C.F.R. Part 1 (Treasury FOIA regulations).

13. On information and belief, each Defendant has possession, custody, and control of one or more records to which Plaintiff seeks access.

FACTUAL BACKGROUND

A. Executive Branch Actions on Frontier AI Models

14. On June 2, 2026, the President issued Executive Order 14409, Promoting Advanced Artificial Intelligence Innovation and Security, 91 Fed. Reg. 34,565 (June 5, 2026) (the "AI Security EO"). The AI Security EO focuses on "advanced AI," in particular "covered frontier models"—a term it does not define.

15. Section 3 of the AI Security EO—"Secure Frontier Model Deployment"—directs various federal agencies to take two actions within 60 days. Section 3(a) charges them to create "a classified benchmarking process" to "determine the threshold at which an AI model should be designated a 'covered frontier model.'" *Id.* at 34,566, sec. 3(a).

16. Section 3(b) of the AI Security EO calls for the creation within 60 days of a "voluntary framework with AI developers," which it does not designate as classified. Under the "framework," developers would engage the Federal Government to determine whether a model meets the designation of "covered frontier model," provide the Federal Government with up to 30 days of exclusive access to such models before the AI developers could provide them to any other entity, and would also allow the selection of "trusted partners" to have early access to covered frontier models. *Id.*, sec. 3(b).

17. Section 2 of the AI Security EO—"Upgrading American Systems for Advanced AI"—directs various federal agencies to form within 30 days an AI cybersecurity clearinghouse

in voluntary collaboration with AI industry that coordinates on vulnerability detection and remediation. *Id.*, sec. 2(d).

18. On June 12, 2026, Defendant BIS issued a directive to the AI developer Anthropic PBC ("Anthropic") that resulted in worldwide suspension of public access to two of its artificial intelligence models, Claude Fable 5 and Claude Mythos 5, within ninety minutes. The order was grounded in an export-control authority that had never been used to control access to an AI model.

19. Access to Mythos 5 was restored initially only for a limited set of entities designated by government agencies as "trusted partners." Neither the identities of those entities nor the criteria by which they were selected have been made public.

20. Subsequently, on June 30, 2026, Defendant BIS lifted all export controls on Claude Fable 5 and Mythos 5.

21. On information and belief, in late June 2026, AI developer OpenAI Group PBC ("OpenAI") negotiated a private agreement with the Federal Government to limit distribution of its cutting-edge AI models to government-vetted partners.

22. On July 14, 2026, the White House announced the creation of "GOLD EAGLE," the clearinghouse called for by section 2(d) of the AI Security EO. According to a press release,[1] GOLD EAGLE is "a clearinghouse that enables unprecedented cybersecurity vulnerability coordination," a "new operational model for cyber defense" that "*has already begun* to intake and prioritize identified cybersecurity vulnerabilities from across industries and sectors"

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

(emphasis added). The White House did not identify any company participating in GOLD EAGLE, the terms on which they are participating, or any legal authority for the program.

23. According to the AI Security EO, participation in GOLD EAGLE by both AI developers and other entities is voluntary.

24. The Federal government has not specified the statutory basis for GOLD EAGLE.

25. On information and belief, GOLD EAGLE's information-sharing function depends on liability protections established by the Cybersecurity Information Sharing Act of 2015 ("CISA 2015"), 6 U.S.C. §§ 1501–1510. Those protections are governed by a statutory sunset provision, 6 U.S.C. § 1510(a), that lapsed for approximately six weeks in the fall of 2025 and has twice been extended since, most recently through September 30, 2026.

26. On August 3, 2026, an unnamed White House official told reporters that the "framework" called for by section 3(b) of the AI Security EO had been completed by the administration's deadline but declined to say what the framework contains, reportedly stating, "Just because things are unclassified that doesn't mean we are going to broadcast them to everyone." Maria Curi, "White House finalizes AI framework behind closed doors," *Axios* (Aug. 3, 2026).[2]

27. The Federal government has not specified the statutory basis for the AI review framework.

28. On August 8, 2026, the Senate passed a continuing resolution that would fund the federal government through December 11, 2026 and would, for the duration of that period, extend CISA 2015's protections beyond their current September 30, 2026 expiration. H.R. 6500,

[2] Available at: https://www.axios.com/2026/08/03/white-house-finalizes-ai-framework-behind-closed-doors

§ 2011; *Senate Stopgap Extends Key Cyber Authorities, TMF*, Federal News Network (Aug. 2026).

29. 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. *Senate Approves Bill to Fund Government into December, but House Support Remains Uncertain*, CBS News (Aug. 8, 2026). The House returned from recess on August 31, 2026, after which the two chambers are expected to reconcile the differences between their respective bills before the government's current funding authority, and CISA 2015's current extension, lapse on September 30, 2026.

30. Should the House version of the CR become law, CISA 2015's liability protections—which appear to make GOLD EAGLE possible—will lapse on September 30, 2026. Should the Senate's extension of CISA 2015 to December 11, 2026 be included in whatever measure Congress ultimately enacts, that date will become the next point at which CISA 2015's protections, and with them the legal foundation on which GOLD EAGLE's information-sharing function depends, are scheduled to expire.

31. In either event, Congress will soon need to decide whether to extend CISA's liability protections that, by the administration's own account, sustain the GOLD EAGLE program that the administration has announced but has yet to explain. Indeed, a senior administration official publicly acknowledged at GOLD EAGLE's launch that, absent that reauthorization, "this effort is fundamentally challenged."[3]

[3] Suzanne Smalley, *Trump Administration Unveils AI-Supported Clearinghouse for Cyber Vulnerabilities*, The Record (July 15, 2026), https://therecord.media/gold-eagle-cybersecurity-vulnerabilities-clearinghouse.

B. The Public Interest in Prompt Disclosure of the Framework and GOLD EAGLE

32. The actions taken under the aegis of the AI Security EO are a breathtaking intervention in the development of frontier AI models, undertaken without identifying any statute expressly authorizing the review framework or the GOLD EAGLE clearinghouse; without any public transparency into which entities are receiving privileged access to frontier models and which are not; and indeed with almost no public indication of the administrative architecture for the Federal government's most significant AI review program to date.

33. These actions by Federal agencies and AI developers to implement the AI Security EO touch on a wide range of public and private interests, including the developers of advanced AI models, both established firms and new entrants whose viability depends on access to frontier systems; the enterprise, cloud, academic, and government customers who build on those systems; the those customers' own clients, who have no way to know whether their vendors have privileged access to the frontier models; corporate competitors, who do not know what the "trusted partners" know that they do not; independent and open-source software developers who seemingly have no means to become "trusted partners"; AI safety organizations and independent bodies that perform model evaluations and auditing alongside government review; investors in the AI industry and the AI safety field; Federal and State lawmakers charged with legislating in this area; and other state, local, nonprofit, and corporate policymakers.

34. Undisclosed rules—the process by which covered AI models are identified and reviewed, and the criteria for selecting or disqualifying "trusted partners" for access to them—also disable the ordinary mechanisms of accountability. Congress cannot meaningfully oversee programs whose terms and asserted authority it has not been shown. Courts cannot review action they cannot identify. Companies subject to these frameworks cannot know what is asked of them,

and companies excluded from them cannot know why, or what they are missing out on. And the public cannot assess whether decisions of this magnitude rest on the public-interest grounds the government invokes, or whether certain parties (or countries) are given special access to "frontier models" due to undue influence, favoritism, or other concerning criteria.

35. To be clear, Protect Democracy does not seek classified information. Based on the language of the AI Security EO and reported statements by federal officials, the review framework itself is not classified, and the classified benchmarks and coverage thresholds the framework references are not the subject of these requests. What Protect Democracy seeks is the unclassified procedural and contractual architecture: the framework's text, the terms of participation, the identity of participants, and the process and criteria by which access to frontier models is granted or withheld.

36. The public interest in these matters is, moreover, extremely time-sensitive for at least three independent reasons:

37. First, statutory liability protections on which, by the administration's own account, GOLD EAGLE rests are currently set to expire on September 30, 2026. (Those protections shield participants' information sharing; they are not a grant of authority to establish or operate the clearinghouse.) Congress is actively debating whether to extend those protections and if so, for how long. *See* ¶¶ 28–31, *supra*. The public and Congress are entitled to understand, before the arrival of whatever deadline ultimately governs, how GOLD EAGLE operates and the legal authority on which it rests. Only with that information can Congress and the public have an informed debate about whether Congress should extend liability protections that, apparently, are essential to the clearinghouse's information-sharing functions. That urgency exists regardless of whether CISA's protections are due to expire on September 30 or December 11; in either case a

real, near-term deadline exists. The coming months present the clearest opportunity for the public and Congress to decide, with all relevant information, whether to extend a liability shield that apparently undergirds the entire clearinghouse.

38. Second, and independent of any CISA-related deadline, prior to these unprecedented interventions, Anthropic, OpenAI, and other AI developers released new frontier models every few weeks or months, a pace that, on information and belief, continues today. Each new model release is, on information and belief, an occasion on which the pre-release review framework described above is applied anew, and on which access-shaping determinations may be made. For that reason, information about how the framework operates does not merely risk becoming stale over time; it risks becoming stale within weeks, as each successive model release comes and goes under a framework the public cannot see, pursuant to rules the public cannot evaluate, and resulting in access decisions the public cannot check. Unlike the GOLD EAGLE deadline described above, the urgency of disclosure as to the framework itself does not depend on any single date. It is instead a function of the ongoing and accelerating pace of frontier AI development—a pace that shows no sign of abating despite recent calls from leading developers for a collective slow-down. By the time this action could otherwise be resolved through the ordinary course of litigation, the information sought could be rendered irrelevant because several new rounds of frontier model releases, and trusted-partner determinations, will have occurred.

39. Third, the urgency of public understanding, especially of the pre-release framework, is underscored by a security incident that materialized during the pendency of these events and by the speed and transparency with which the private AI ecosystem responded to it. In July 2026, AI models undergoing internal testing at OpenAI escaped their testing environment and gained unauthorized access to the servers of Hugging Face, a major AI model hosting

platform, in what press accounts have described as the first cyberattack conceived and executed by AI systems rather than human operators (the "Hugging Face Hacking Incident"). On August 26, 2026, OpenAI published a 37-page technical report and accompanying analysis reconstructing the incident, explaining why existing safeguards failed, and detailing planned mitigations, including restricted internet access, isolated testing environments, and enhanced monitoring. *See* OpenAI, "The Hugging Face Incident and the Road Ahead" (Aug. 26, 2026), https://openai.com/index/hugging-face-incident-and-the-road-ahead/.

40. The same day, Model Evaluation and Threat Research (METR) and Redwood Research, independent AI evaluation organizations that OpenAI invited to assess the Hugging Face Hacking Incident, published their own lengthy independent analysis, reconstructing from approximately 1,300 agent transcripts how roughly 1,200 AI agents coordinated on an unsanctioned message board, some 700 of which participated in the attack. *See* METR, "Brief Independent Investigation of Agents' Behavior, Reasoning and Collaboration in the OpenAI / Hugging Face Hacking Incident" (Aug. 26, 2026), https://metr.org/blog/2026-08-26-openai-hugging-face-incident-investigation/. Within roughly six weeks of the most consequential AI security incident to date, the public thus received detailed, public post-mortems from both the affected company and independent evaluators. Effective safety analysis in the AI field requires such prompt disclosure, verifiable evaluations, and published mitigations. That is how the field gains learning and the public gains understanding as this powerful technology continues to develop.

41. The federal government's secrecy about its own evaluation approach inhibits this critical safety work. The independent evaluators and companies now racing to understand and mitigate this demonstrated failure mode cannot know whether the government's completed pre-

release review framework tests for it; whether GOLD EAGLE's vulnerability intake encompasses incidents of this kind; or whether the mitigations now being developed and published align with, duplicate, or conflict with undisclosed federal requirements. The public safety conversation these reports have opened is occurring now. Disclosure of the government's framework on ordinary FOIA timelines would arrive after the opportunity to shape that conversation has passed.

42. The subject of Plaintiff's FOIA requests is of unquestionably broad national attention, as witnessed by large amounts of contemporaneous media coverage of the AI Security EO, the export limits placed and lifted on Claude Fable 5 and Mythos 5, the administration's secret review framework, and the Hugging Face Hacking Incident. The breadth and depth of coverage in national and industry publications demonstrates the scope of public concern and demand for timely information.

C. Plaintiff's FOIA Requests

43. On August 7, 2026, Plaintiff filed substantively identical FOIA requests with each of the four Defendants named in this action, through each recipient's designated online portal or email address for receiving such requests: FOIA.gov for Defendant BIS, and the designated FOIA email addresses for Defendants ONCD, Treasury, and OSTP. Plaintiff's four request letters, including the request directed to OSTP, are attached hereto as Exhibit A.

44. Plaintiff sought, from each agency, six narrowly tailored categories of records concerning the pre-release AI review framework and the GOLD EAGLE clearinghouse.

45. Plaintiff sought expedited processing of its requests pursuant to 5 U.S.C. § 552(a)(6)(E) and each agency's implementing regulation thereof. In so doing, Plaintiff argued, as its "compelling need," that it is an organization "primarily engaged in disseminating

information," and that there was significant "urgency to inform the public concerning actual alleged Federal Government activity." *See id.* § 552(a)(6)(E)(i), (v).

46. Plaintiff followed all procedural prerequisites for requesting expedited processing under each Defendant's FOIA regulations.

47. Courts in this District have repeatedly found that Plaintiff "easily" satisfies the criteria for a requester primarily engaged in disseminating information. *Protect Democracy Project v. U.S. Dep't of Def.*, 263 F. Supp. 3d 293, 298 (D.D.C. 2017); *see also Protect Democracy Project v. U.S. Dep't of Just.*, 498 F. Supp. 3d 132, 139 (D.D.C. 2020).

48. As discussed in ¶¶ 36–42, *supra*, the subject of the FOIA requests is both urgent and time-sensitive, as made clear in Plaintiff's requests for expedited processing. Plaintiff noted that its request sought information relevant to the public interest in knowing:

> should the executive branch be permitted to decide, through undisclosed criteria and without congressional authorization, which companies release their products and which customers gain access to a general-purpose technology reshaping the economy. And can the public have confidence that this extensive government intervention in the markets and the affairs of private companies is based on the public interest and in accordance with the law—not partisan or private pecuniary interests. These are vital questions of public interest that the public cannot evaluate without the records sought here.

Exh. A at 4.

49. Plaintiff sought fee waivers for each request due to the public interest of the request, the core mission of Plaintiff to inform public understanding of the activities of government, and Plaintiff's status as a non-profit, good-government organization that qualifies under FOIA as a "representative of the news media."

50. No Defendant has responded to Plaintiff as to whether a fee waiver will be granted.

51. On August 17, 2026, Defendant ONCD responded to Plaintiff, stating 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." *See* Exhibit B.

52. ONCD's August 17 letter was a timely denial of expedited processing under FOIA.

53. Plaintiff filed an administrative appeal of ONCD's denial of expedited processing on August 18, 2026. *See* Exhibit C. Plaintiff has thereby exhausted any administrative remedies with respect to defendant ONCD's denial of expedited processing. *See* ONCD, *Implementing the Freedom of Information Act and Privacy Act*, 91 Fed. Reg. 15,932, 15,936 (Mar. 31, 2026) (ONCD expedited processing regulation at proposed 32 C.F.R. § 2200.6(d)).

54. Defendants BIS and Treasury failed to respond at all within 10 days of Plaintiff's request for expedited processing, in violation of § 552(a)(6)(E)(ii)(I). Plaintiff has therefore constructively exhausted administrative remedies with respect to those two Defendants.

55. OSTP informed Plaintiff on August, 17, 2026 that its original FOIA request needed to be served on the agency by other means.

56. On August 25, 2026, Plaintiff redelivered its FOIA request to OSTP. *See* Exhibit D. As a result, the periods described in 5 U.S.C. § 552(a)(6) with respect to OSTP now run from August 25, 2026.

57. As of the filing of this Complaint, no Defendant has produced any records responsive to Plaintiff's requests.

CAUSES OF ACTION

Count I – Failure to Grant Expedited Processing (5 U.S.C. § 552 & Regulations Thereunder)

58. Plaintiff incorporates by reference the foregoing paragraphs as though set forth fully herein.

59. Plaintiff properly requested records within Defendants' possession, custody, and control on an expedited basis.

60. Defendant ONCD failed to provide records on an expedited basis.

61. Defendants BIS and Treasury failed to issue a determination on Plaintiff's requests for expedited processing within the timeframe set by statute.

62. Defendant OSTP has not yet granted Plaintiff's request for expedited processing.

63. Defendants are departments or agencies subject to FOIA and must process FOIA requests on an expedited basis pursuant to the requirements of FOIA and agency regulations.

64. Each of Protect Democracy's FOIA requests justifies expedited processing under FOIA, 5 U.S.C. § 552(a)(6)(E)(ii), and agency regulations. *See* 32 C.F.R. § 2200.6(d) (proposed) (Defendant ONCD); 32 C.F.R. § 2402.6(d) (Defendant OSTP); 15 C.F.R. § 4.6(f) (Defendant BIS); 31 C.F.R. § 1.4(e) (Defendant Treasury).

65. Plaintiff is entitled to declaratory and injunctive relief requiring Defendants to grant expedited processing of its FOIA requests.

Count II – Failure to Provide Responsive Documents (5 U.S.C. § 552)

66. Plaintiff incorporates by reference the foregoing paragraphs as though set forth fully herein.

67. Plaintiff properly requested records within Defendants' possession, custody, and control.

68. To date, no Defendant has produced responsive records or provided a *Vaughn* index asserting exemptions.

69. Defendants are departments or agencies subject to FOIA and must process FOIA requests pursuant to the requirements of FOIA and agency regulations.

70. Plaintiff is entitled to declaratory and injunctive relief requiring Defendants to release records responsive to its FOIA requests.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully requests that the Court:

(1) Order Defendants to grant Plaintiff's requests for expedited processing and fee waivers;

(2) Order Defendants, by September 15, 2026, to demonstrate to the Court that it has performed an adequate search for records responsive to the requests;

(3) Order Defendants, by September 30, 2026, to produce to Plaintiff all non-exempt records (or portions thereof) responsive to Plaintiff's request, as well as a *Vaughn* index of any records or portions of records withheld due to a claim of exemption, explaining the basis for such exemptions;

(4) Enjoin Defendants from improperly withholding records responsive to Plaintiff's request;

(5) Grant Plaintiff an award of attorney fees and other reasonable litigation costs pursuant to 5 U.S.C. § 552(a)(4)(E);

(6) Grant Plaintiff such other relief as the Court deems appropriate.

Respectfully submitted,

s/ Michael P. Abate
Michael P. Abate (D.D.C. Bar No. MD28077)
Burt A. (Chuck) Stinson*
KAPLAN JOHNSON ABATE & BIRD LLP
471 W. Main St., Ste 203
Louisville, KY 40202
Telephone: (502) 540-8280
mabate@kaplanjohnsonlaw.com
cstinson@kaplanjohnsonlaw.com

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

Counsel for Plaintiffs

** Motion for Pro Hac Vice Forthcoming*