Form A1-1. Motion for Entry of a Protective Order Governing Classified Information (Civil)

> **Instructions page. Delete this page before use.** Sample template for use by or with a licensed attorney. Not legal advice. Laws differ by jurisdiction and change; adapt the document to your facts and check every citation before relying on it. Version 1.10, October 2026. Legal information, not legal advice. Published by the Emergent Frontiers Institute (NHI Law is not a law firm). Citations checked in October 2026; check every citation before relying on it. Web version: https://nhilaw.com/forms/a1-1.html

Use. A plaintiff in a civil action that will involve classified information (for example, a reprisal, tort, contract, or constitutional claim arising from a UAP-related program) moves early, before the government asserts the state secrets privilege, for a protective order that lets cleared counsel review classified material under secure conditions. Early entry of such an order supports a later argument that the case can be litigated without dismissal, because the court will already have procedures for handling the material. See *In re Sealed Case*, 494 F.3d 139 (D.C. Cir. 2007); *Al Shimari v. CACI Premier Technology, Inc.*, 170 F.4th 162 (4th Cir. 2026).

When to use. A civil case in which classified information will be produced or relied on, or in which the government has signalled a state secrets assertion. Move before discovery starts. **Not for:** Criminal cases, where CIPA §3 governs (Form A2-2).

Deadlines. None set by statute. Seek entry before the first production; a later order may not reach material already withheld.

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

[PLAINTIFF], Plaintiff, v. [DEFENDANT AGENCY / OFFICIAL / CONTRACTOR], Defendants.	Civil Action No. [_____] ([Judge initials]) **PLAINTIFF'S MOTION FOR ENTRY OF A PROTECTIVE ORDER GOVERNING CLASSIFIED INFORMATION AND FOR SECURITY CLEARANCE PROCESSING OF PLAINTIFF'S COUNSEL**

Plaintiff [name] moves under Federal Rule of Civil Procedure 26(c) and the Court's inherent authority to manage its docket for entry of the attached proposed Protective Order governing the handling of classified information in this action, and for an order directing Defendants to initiate security clearance processing for Plaintiff's counsel of record. Pursuant to Local Civil Rule 7(m), counsel for Plaintiff conferred with counsel for Defendants on [date] by [method]. Defendants [oppose / take no position / consent in part, as follows: _____].

MEMORANDUM OF POINTS AND AUTHORITIES

I. Background

This action arises from [brief description: e.g., Defendants' alleged reprisal against Plaintiff for disclosures to the All-domain Anomaly Resolution Office protected by 50 U.S.C. § 3373b; or injuries Plaintiff sustained in the course of work at (facility)]. Plaintiff anticipates that discovery, and possibly Defendants' defenses, will involve information that Defendants consider classified, including [general categories stated without classified detail, e.g., the identity of program offices, internal reporting records, security classification guides].

Much of the subject matter of this case has been officially acknowledged. [List official acknowledgments with citations: statutory provisions (e.g., 50 U.S.C. §§ 3373, 3373b; Pub. L. No. 118-31, §§ 1841-1843); sworn testimony of officials before Congress (hearing, date, witness, page); agency reports (title, date); records released by the Department of War or the

National Archives (identifier, date).] Those acknowledgments matter here because the protection the law gives to national security information turns on official confirmation. See *United States v. Zubaydah*, 595 U.S. 195, 210-11 (2022).

Plaintiff's counsel, [name(s)], [hold / have previously held / are eligible to apply for] security clearances at the [level] level. [Describe prior clearance history if any, without classified detail.]

II. Argument

A. The Court has authority to enter a protective order governing classified information in a civil case.

Rule 26(c) authorizes the Court, for good cause, to issue an order "specifying terms … for the disclosure or discovery" of information and requiring that information "be revealed only in a specified way." The Classified Information Procedures Act, 18 U.S.C. App. 3, applies by its terms only to criminal prosecutions, but courts in civil cases routinely adopt protective orders modeled on CIPA § 3 and on the procedures used in national security habeas litigation in this District. *See In re Guantanamo Bay Detainee Litigation*, 577 F. Supp. 2d 143 (D.D.C. 2008) (entering protective order for classified information in consolidated habeas cases; counsel presumed to have a "need to know" information in their own and related cases), *amended* (D.D.C. July 10, 2009). The Court of Federal Claims has published guidelines for the same purpose. U.S. Court of Federal Claims, *Guidelines for Classified Information* (Apr. 2021).

B. Entry of the order now will allow the case to proceed on the merits.

The state secrets privilege belongs to the government and must be asserted formally by the head of the department with control over the matter, after personal consideration. *United States v. Reynolds*, 345 U.S. 1, 7-8 (1953). If Defendants assert it, the ordinary consequence is the removal of the privileged evidence from the case, and the case proceeds. *In re Sealed Case*, 494 F.3d at 144-45. Dismissal is reserved for the exceptional case in which the plaintiff cannot make out a prima facie case without privileged evidence, the privilege deprives the defendant

of a valid defense, or privileged and nonprivileged evidence cannot be separated. *Mohamed v. Jeppesen Dataplan, Inc.*, 614 F.3d 1070, 1083 (9th Cir. 2010) (en banc). Whether a case reaches that point depends heavily on the protective measures the court has available. In *Al Shimari v. CACI Premier Technology, Inc.*, the Fourth Circuit reasoned that a contractor was not prejudiced by the privilege where the district court had used pseudonymous and telephonic testimony and other measures, and the case was tried to verdict. 170 F.4th 162, 197-98 (4th Cir. 2026), vacated on reh'g on other grounds, 2026 WL 2547096 (4th Cir. Aug. 28, 2026) (per curiam) (unpublished). A protective order entered at the outset gives the Court those tools before any dispute arises.

C. Counsel's clearance processing should begin now.

Clearance processing takes months. Starting it now avoids delay later and allows counsel to receive classified filings, attend any closed hearing, and review classified declarations to the extent the Court permits. Clearance alone does not confer access; the classifying agency must also find a need to know. The proposed order therefore asks the Court to direct Defendants to submit counsel's applications promptly and to report any need-to-know determination to the Court, so that the Court can resolve disputes about access.

D. The proposed order protects national security.

The proposed order requires storage of classified material in a facility approved by the Classified Information Security Officer (CISO); prohibits disclosure except to cleared persons with a need to know; requires filing of classified material with the CISO; provides for classification review of Plaintiff's filings before public filing; and provides for sanctions. These measures are drawn from orders that courts have used for years without compromise of classified information.

III. Conclusion

The Court should enter the attached Protective Order and direct Defendants to begin security clearance processing for Plaintiff's counsel within [14] days.

Dated: [_____] Respectfully submitted,

[signature block]

[PROPOSED] PROTECTIVE ORDER GOVERNING CLASSIFIED INFORMATION

Upon consideration of Plaintiff's Motion, and for good cause shown, it is ORDERED:

1. **Scope.** This Order governs all classified information, and all information that a party reasonably believes may be classified, that is produced, filed, or otherwise used in this action. "Classified information" means information classified under Executive Order 13526 or any successor order, or under the Atomic Energy Act of 1954, and includes information in any form bearing classification markings or that a party has been notified is classified.

2. **Classified Information Security Officer.** The Court designates [name], of the Department of Justice Litigation Security Group, as CISO, with [name] as alternate. The CISO shall advise the Court and the parties on security procedures and shall not disclose to any party the substance of another party's classified filings.

3. **Clearances.** Within [14] days, Defendants shall submit to the appropriate agency the security clearance applications of Plaintiff's counsel of record [and named staff and experts]. Defendants shall report the status of each application to the Court every [30] days. Any determination that a cleared person lacks a need to know specific information shall be reported to the Court, which may resolve the dispute after ex parte, in camera review if necessary.

4. **Access.** No person shall have access to classified information under this Order unless that person holds an appropriate clearance, has been determined to have a need to know, and has signed the Memorandum of Understanding attached as Exhibit A.

4A. **Experts and consultants.** A party may designate experts or consultants who need access to classified information to assist counsel. The designating party shall submit each designee's name to the CISO for clearance processing under paragraph 3. No designee shall have access before being cleared, determined to have a need to know, and signing Exhibit A.

5. **Secure area.** Classified information shall be stored, reviewed, and processed only in a secure area approved by the CISO. Counsel may prepare classified filings only in the secure area on equipment approved by the CISO.

6. **Filing.** Classified filings shall be submitted to the CISO, who shall deliver them to the Court and to cleared counsel for the other parties. Each party shall file a public version with classified material redacted after classification review under paragraph 7.

7. **Classification review.** Any filing, transcript, or other document that may contain classified information shall be submitted to the CISO for classification review before public filing. Defendants shall complete review within [7] days unless the Court orders otherwise.

8. **Official acknowledgment.** Information that has been officially acknowledged by the United States (including information contained in statutes, public reports to Congress, sworn public testimony of federal officials, and records released by an agency or the National Archives) may be used in unclassified filings and proceedings without classification review, provided that the filing identifies the source of the acknowledgment. A party that believes particular information is not officially acknowledged may raise the matter with the Court. [Note: expect the government to oppose this paragraph; it is included to frame the official-acknowledgment issue early.]

9. **Hearings.** Proceedings at which classified information may be disclosed shall be closed to persons not authorized under this Order. Transcripts shall be reviewed under paragraph 7.

10. **Pseudonyms and substitutes.** The parties shall meet and confer about pseudonyms for witnesses whose identities are classified, unclassified summaries, and stipulations, and shall present any disagreement to the Court.

11. **No waiver.** Nothing in this Order waives any privilege, including the state secrets privilege, or constitutes a determination that any information is or is not classified or privileged.

12. **Return or destruction.** At the conclusion of this action, classified information shall be returned to the CISO.

13. **Sanctions.** Violation of this Order may result in sanctions, including contempt, and may constitute a violation of criminal law.

SO ORDERED.

Dated: [_____] _____ United States District Judge

Exhibit A. Memorandum of Understanding Regarding Receipt, Storage, and Handling of Classified Information

I, [name], agree as follows:

1. I have been given access, or may be given access, to classified information in connection with [caption, Civil Action No. ____] (the "Action") under the Protective Order entered by the Court on [date].

2. I will not disclose classified information to any person except (a) the Court, (b) a person who holds the appropriate clearance, has been determined to have a need to know, and has signed this Memorandum, and (c) as the Protective Order otherwise permits. I will not disclose classified information to my client unless the client provided it, or the Court orders otherwise.

3. I will review, discuss, store, and prepare documents containing classified information only in the secure area approved by the Classified Information Security Officer, using only equipment the CISO has approved.

4. I will submit any document that I believe may contain classified information to the CISO for classification review before filing it publicly or providing it to any person not authorized to receive it.

5. I will not use classified information obtained in the Action for any purpose other than the Action.

6. I understand that my obligations continue after the Action ends, that I must return all classified information to the CISO at the end of the Action, and that unauthorized disclosure may violate federal criminal law, including 18 U.S.C. §§793, 798, and 1924, and may be punished as contempt of court.

7. I have read the Protective Order and agree to be bound by it. I consent to the Court's jurisdiction to enforce this Memorandum.

[Signature] [Date]

[Printed name; organization; role in the Action]

Drafting notes

- Confirm current local practice with the CISO before filing; Litigation Security Group procedures change.
- In a contractor-only case (no federal defendant), the government may intervene or file a statement of interest. Serve the U.S. Attorney and consider notice under 28 U.S.C. § 517.
- If the case is in the Court of Federal Claims, cite the Court's 2021 *Guidelines for Classified Information* and RCFC 26(c).
- Do not attach or describe anything that may be classified. Counsel who receives information that may be classified from a client should contact the CISO or the agency's security office before using it.