

Form B4-2. Newsroom and Website Protocol for Receiving and Publishing UAP Material That May Be Classified

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/b4-2.html>

When to use. Newsrooms, authors, producers, podcasters, and websites that may receive classified or sensitive UAP material. **Not for:** Material the organization has solicited, which raises different risks.

Deadlines. Apply the moment material arrives; counsel within 24 hours of any subpoena or warrant.

1. Purpose. To report on UAP while limiting legal risk to the organization, its staff, and sources under 18 U.S.C. §§793 and 798, the Atomic Energy Act, and defamation law, and to protect sources.

2. Do not solicit. Staff shall not ask any person to provide documents or information that the person is not authorized to disclose. Staff may ask sources what they are free to say and may tell sources about protected channels (50 U.S.C. §3373b; inspector general and congressional whistleblower channels) and about the value of counsel.

3. Receipt of marked or apparently classified material.

- (a) Do not forward, copy, or upload the material to shared systems.
- (b) Notify [the editor-in-chief and counsel] the same day.
- (c) Record how, when, and from whom (if known) the material arrived. Do not pay for it.
- (d) Store any physical copy in a locked location with access limited to staff assigned to the story.
- (e) Counsel will advise whether to retain, return, or destroy the material and whether any reporting obligation applies.

4. Assessment before publication. Before publishing material or information that may be classified, the editor and counsel shall consider:

- (a) whether the information is already officially acknowledged (statutes, AARO reports, official releases, sworn testimony of officials) and can be sourced to those acknowledgments;
- (b) whether it includes communications intelligence (18 U.S.C. §798), Restricted Data (42 U.S.C. §2014(y)), or identities of covert personnel (50 U.S.C. §3121), which carry heightened risk;
- (c) whether details such as names of junior personnel, locations of facilities, platform and sensor data, or program code words can be omitted without loss to the story;
- (d) whether the government's closely held confirmation of a public report is itself the sensitive element (*United States v. Rosen*, 445 F. Supp. 2d 602 (E.D. Va. 2006)); and
- (e) whether to seek comment from the agency, and what to tell it.

5. Source protection. Use secure communication tools; minimize retention of identifying information; do not reveal source identities to anyone outside the assigned team; consider state shield laws and the absence of a federal shield statute. Counsel shall be consulted promptly about any subpoena, warrant, or request for records, and staff shall not hand over notes or devices without counsel.

- (a) *Privacy Protection Act.* Officers investigating a crime generally may not search for or seize a publisher's work product or documentary materials (42 U.S.C. §2000aa). The protection does not apply where the publisher is suspected of receiving, possessing, or communicating national defense or classified information in violation of 18 U.S.C. §§793, 794, 797, or 798 (§2000aa(a)(1)), so it gives little protection once the organization holds classified material.
- (b) *DOJ news-media policy.* Federal subpoenas and warrants for news-media records are governed by 28 C.F.R. §50.10, as revised May 2, 2025 (90 Fed. Reg. 18786), which withdrew the 2022 protections. Assume reporters' phone, email, and cloud records can be sought in a leak investigation, and choose tools and retention practices accordingly.
- (c) *Reporter's privilege.* There is no First Amendment or common-law privilege for a reporter to refuse to name a source at a federal leak trial in the Fourth Circuit. *United States v. Sterling*, 724 F.3d 482 (4th Cir. 2013).
- (d) *State shield laws.* [For California staff:] California's shield law (Cal. Const. art. I, §2(b); Evid. Code §1070) protects against contempt for refusing to disclose a source or unpublished information

in California proceedings. It does not protect against federal process. [Insert the shield law of each state where staff work.]

6. Allegations about named people and companies. Allegations that named officials or contractors concealed programs, misled Congress, retaliated against witnesses, or harmed anyone require: (a) at least two independent sources or documentary support; (b) a request for comment; (c) attribution language (“X stated under oath that...”) rather than assertion; and (d) counsel review. See [Issue G1](#).

7. Corrections. Errors shall be corrected promptly and transparently.

8. Training. All staff working on UAP stories shall review this protocol annually.