

Protecting UAP Whistleblowers: Statutory Channels, Reprisal Remedies, Clearance Risk, and the PURSUE Waiver

Version 1.10 · October 2026 · nhilaw.com/issues/cl.html

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.

Key points

- Protection runs only through specific channels; the choice of channel decides whether the client is protected.
 - The AARO mechanism (50 U.S.C. §3373b) is the only channel with statutory criminal protection. On the site's premise that AARO is part of the concealment, use it for that protection, keep the disclosure to AARO minimal, and make the substantive disclosure in parallel to an inspector general and the committees.
 - PURSUE (Sept. 14, 2026) waives only civil and administrative NDA enforcement for communications to the PURSUE team.
 - Clearance actions are largely unreviewable in court (*Egan*; *Lee v. Garland*); the remedy is the §3341(j) process, with strict deadlines.
 - Contractor employees have additional remedies that are often overlooked: 10 U.S.C. §4701, False Claims Act retaliation (31 U.S.C. §3730(h)), Sarbanes-Oxley (18 U.S.C. §1514A), and DTSA immunity for reports to officials (18 U.S.C. §1833(b)).
 - Referring a service member for a mental-health evaluation as reprisal is prohibited (DoDI 6490.04 ¶3.e).
-

1. Summary

A current or former government or contractor employee with knowledge of UAP programs has more legal protection in 2026 than at any earlier time, but the protection runs only through specific channels. The choice of channel decides whether the client is protected.

Channel	Who may use it	Legal effect	Limits
AARO authorized	Current and former	Disclosure “shall not	Disclosure to AARO

Channel	Who may use it	Legal effect	Limits
reporting mechanism , 50 U.S.C. §3373b	federal employees, contractors, and others with UAP information	be subject to a nondisclosure agreement,” is deemed to comply with EO 13526 and Atomic Energy Act rules, and “is not a violation of section 798 of title 18, or other provision of law relating to the disclosure of information”; reprisal prohibited (§3373b(b))	only; public disclosure not authorized; enforcement of reprisal ban through procedures “consistent with” 10 U.S.C. §1034 and 50 U.S.C. §3234. On the site’s premise that AARO is part of the concealment, the channel gives legal protection but no assurance that AARO will act on, preserve, or protect the disclosure
PURSUE waiver (Department of War, Sept. 14, 2026)	Current and former DoW service members, civilians, and contractors with UAP-related national defense information	“Supersedes civil and administrative enforcement provisions” of NDAs and SAP indoctrination agreements “strictly for communications directed to the PURSUE team”	No stated criminal protection; no public disclosure; covers DoW agreements; information remains subject to security review
ODNI NDA-waiver guidance (July 31, 2026)	IC employees (contractor procedures pending)	NDAs barring disclosure to the President, PURSUE, or designees no longer in force for that purpose	Agency guidance, not law; no public disclosure or congressional disclosure outside existing channels
IC whistleblower channels (50 U.S.C. §3033(k)(5) urgent concern; PPD-19; 50 U.S.C. §3234; §3341(j))	IC employees and (for some provisions) contractors	Protected disclosures to IGs and, through the ICIG, to the intelligence committees; anti-reprisal for personnel and clearance actions	Remedies are administrative (IG review, External Review Panel); limited judicial review
DoD military and civilian channels (10	Service members; civil servants; DoD, NASA,	Reprisal remedies through IG, OSC,	Classified disclosures must go to authorized

Channel	Who may use it	Legal effect	Limits
U.S.C. §1034; 5 U.S.C. §2302(b)(8)-(9); 10 U.S.C. §4701 for contractors)	Coast Guard contractor employees	MSPB, Board for Correction, or district court (contractors after exhaustion)	recipients
Congress directly	Anyone	Members and committees can receive classified information only in proper channels	Disclosure to members outside committee channels is not clearly protected

The main dangers are clearance revocation and criminal exposure. Clearance decisions are largely beyond judicial review (*Department of the Navy v. Egan*, 484 U.S. 518 (1988); *Lee v. Garland*, 120 F.4th 880 (D.C. Cir. 2024)), so the statutory clearance-reprisal process (50 U.S.C. §3341(j)) is the main remedy. A district court has allowed procedural and retaliation challenges to a summary, process-free revocation to proceed (*Zaid v. Executive Office of the President*, 815 F. Supp. 3d 113 (D.D.C. 2025), appeal filed (D.C. Cir. Jan. 13, 2026)). Criminal exposure is removed for disclosures to AARO under §3373b(b)(1)(C), but not for disclosures to the press, to unauthorized persons, or (on the waiver's terms) for anything beyond civil and administrative NDA enforcement in PURSUE communications.

Practical rule. Route classified UAP disclosures through §3373b first, because it carries statutory criminal protection, and treat that disclosure as a legal act and not as a request for action. The site's working premise is that AARO is a deliberate disinformation source and part of the concealment, and a former director of the Navy's UAP Task Force has called it "really a front for the Legacy Program" (Jay Stratton, *Out of the Shadows* ch. 62 (2026)). On that premise:

1. disclose to AARO only what is needed to secure the protection, and keep a dated record of exactly what was said;
2. make the substantive disclosure in parallel to an inspector general (the employing agency's IG, the DoD IG, or the ICIG) and, through the ICIG urgent-concern process, to the intelligence committees;
3. ask the committees, through a member's office, to confirm that AARO sent the 72-hour notification §3373b(a)(4)(B) requires when the disclosure concerns an unreported program;
4. assume that what the client tells AARO may reach the program the client is reporting on, and plan for reprisal from the first day (§§4-5 below); and
5. use PURSUE in addition if the client is or was in the Department of War.

Document everything, and never let a client disclose classified information publicly or to a journalist.

2. The §3373b mechanism in detail

Text. 50 U.S.C. §3373b(a)(1) requires the Secretary of Defense, acting through AARO and in consultation with the DNI, to “establish a secure mechanism for authorized reporting of (A) any event relating to unidentified anomalous phenomena; and (B) any activity or program by a department or agency of the Federal Government or a contractor of such a department or agency relating to unidentified anomalous phenomena, including with respect to material retrieval, material analysis, reverse engineering, research and development, detection and tracking, developmental or operational testing, and security protections and enforcement.”

Handling. Disclosures are administered by cleared personnel, shared promptly with AARO regardless of classification, and, where they concern a restricted, special, or compartmented access program not “explicitly and clearly reported” to the defense and intelligence committees, reported to those committees within 72 hours (§3373b(a)(4)). AARO must publish guidance on accessing the mechanism (§3373b(a)(5)(B)).

Protections (§3373b(b)). - (b)(1): no NDA applies to the disclosure; it is deemed compliant with EO 13526 and Atomic Energy Act chapter 18 rules; and it “is not a violation of section 798 of title 18, or other provision of law relating to the disclosure of information.” This reaches 18 U.S.C. §793, 798, 1924, and 50 U.S.C. §3121 to the extent they concern disclosure. - (b)(2): federal and contractor officials with personnel authority may not take or threaten personnel actions in reprisal; enforcement procedures are to be consistent with 10 U.S.C. §1034, 50 U.S.C. §3234, “or other similar provisions of law regarding prohibited personnel actions.”

Who is covered. The text protects “an individual” making an authorized disclosure, which covers current and former employees, contractors, service members, and others.

Practice points. 1. Confirm, in writing, that the channel used is the §3373b “mechanism for authorized reporting” (AARO’s published guidance; a designated cleared AARO representative). Informal contact with an AARO employee may not qualify. 2. Disclose only to the mechanism; any onward disclosure (to the press or others) falls outside the protection. 3. Keep a record of what was disclosed, when, and to whom, through cleared counsel if possible. 4. Reprisal enforcement depends on implementing procedures. Section 3373b(b)(2)(B) directs the Secretary of Defense and the DNI to “establish procedures for the enforcement” of the reprisal ban “consistent with, as appropriate, section 1034 of Title 10, section 3234 of this title, or other similar provisions of law.” A search on October 14, 2026 found no published procedures (no Federal Register notice and nothing on AARO’s public site beyond the reporting guidance and contact form). The closest DoD statement is AARO’s “UAP Self Reporting Mechanism User Guide” (Nov. 2023), cleared by DOPSR on December 11, 2023 for posting on aaro.mil and released under FOIA as DoD 25-F-3452. It tells reporters that “[i]ndividuals who make authorized disclosures to AARO are explicitly protected from reprisal,” directs anyone who experiences reprisal to the DoD, ICIG, DOE, or DHS inspector general hotlines “or the IG office of your current or former federal agency,” and states that “other than authorized disclosures made to AARO,” individuals remain bound by their nondisclosure agreements. It also limits the web form to firsthand knowledge of government programs dating back to 1945, excludes classified information and current operational sightings, and promises a possible follow-up

interview “in an appropriate setting.” Referral to an inspector general hotline is a complaint channel and does not supply the enforcement procedures §3373b(b)(2)(B) requires. Ask AARO and the employing agency in writing for the procedures, and in the meantime preserve the parallel remedies: 10 U.S.C. §1034 for service members, 50 U.S.C. §3234 and PPD-19 for intelligence community employees, 50 U.S.C. §3341(j) for clearance actions, and 10 U.S.C. §4701 for contractor employees.

3. The PURSUE waiver

Source. Department of War press release, “Department of War Issues Legal Waiver to Authorize Unidentified Anomalous Phenomena (UAP) Disclosures to PURSUE” (Sept. 14, 2026). The underlying waiver instrument has not been published; the release is the only public text located. The PURSUE program itself rests on the President’s February 19, 2026 statement directing the Secretary of War and other agencies “to begin the process of identifying and releasing government files related to alien and extraterrestrial life, unidentified aerial phenomena (UAP), and unidentified flying objects (UFOs),” as reproduced on war.gov/UFO.

What the release says. - Covered persons: “all current and former DOW service members, civilian personnel, and contractors holding or previously granted access to UAP-related National Defense Information (NDI).” - Authorization: they “are authorized to disclose protected information directly to official PURSUE representatives.” - Effect: the waiver “supersedes civil and administrative enforcement provisions contained within Non-Disclosure Agreements (NDAs) and Special Access Program Indoctrination Agreements (SAPIAs) previously executed within the United States, strictly for communications directed to the PURSUE team,” and authorizes disclosures “without triggering breach-of-agreement penalties or standard NDA violations.” - Purpose: an “authorized pipeline for systematic review, security evaluation, and potential declassification.”

What it does not say. - It does not purport to waive criminal statutes. Because the disclosure is “authorized,” a later prosecution under §793 for the same communication would face strong defenses (the communication was to a person “entitled to receive it,” and authorization defeats willfulness), but the release does not say so and a press release cannot amend a statute. - It does not cover NDAs executed with other agencies (CIA, NSA, NRO, DOE), except to the extent those agencies adopt parallel waivers (ODNI’s July 31, 2026 guidance points that way for IC agencies). - It does not authorize public disclosure or disclosure to Congress. - It does not address collateral classified information that is inseparable from the UAP information. - It does not establish reprisal remedies beyond those already in law.

Enforceability. A press release describing an agency waiver is evidence of the agency’s position and supports reliance and estoppel-type arguments in any later administrative action, but it is not a regulation and may be withdrawn. Counsel should request a copy of the signed waiver instrument and the implementing guidance before advising reliance, and should prefer §3373b where both are available.

Relationship to §3373b. The two channels can be used together. §3373b provides statutory criminal protection and anti-reprisal duties; PURSUE provides a route into the declassification and release process. A prudent sequence is: disclose through §3373b; then, if the client wants the

information considered for release, communicate with PURSUE representatives, referencing the §3373b disclosure.

4. Reprisal remedies by type of employee

4.1 Intelligence community employees

- **PPD-19** (Oct. 10, 2012), codified in part at 50 U.S.C. §3234 (prohibited personnel practices in the IC) and 50 U.S.C. §3341(j) (retaliatory revocation of security clearances and access determinations).
- **Process for clearance reprisal (50 U.S.C. §3341(j)).** (1) Within 90 days after notice of an adverse clearance or access decision, the employee or former employee may appeal within the agency (tollable for lack of notice or factors beyond the employee's control); there is no appeal of a suspension for purposes of conducting an investigation. (2) The agency must find a violation if a protected disclosure "was a contributing factor" unless it shows by a preponderance of the evidence it would have acted anyway, "giving the utmost deference to the agency's assessment" of the security threat. (3) Corrective action may include back pay, related benefits, travel expenses, and compensatory damages. (4) Within 60 days after an adverse final agency determination, the employee may appeal to the Director of National Intelligence under DNI procedures; the DNI notifies the intelligence committees of orders on appeal. (5) "Nothing in this section shall be construed to permit or require judicial review of any (A) agency action under this section; or (B) action of the appellate review procedures established under paragraph (5)." §3341(j)(6). (6) Nor does the section create "a private cause of action to challenge the merits of a security clearance determination." §3341(j)(7). Personnel actions (as opposed to clearance actions) follow 50 U.S.C. §3234 and agency and ICIG procedures, including External Review Panels.
- **Judicial review.** Generally unavailable. Courts have declined to review clearance decisions (*Egan*), and the D.C. Circuit holds that constitutional challenges to clearance revocations are nonjusticiable (*Lee v. Garland*, 120 F.4th 880 (D.C. Cir. 2024)). The Federal Circuit has held that the MSPB lacks jurisdiction over an employee's attempt to "bring back" PPD-19 claims as an individual right of action appeal without first exhausting before the Office of Special Counsel. *Akerman v. MSPB*, 2025 WL 1140194 (Fed. Cir. Apr. 15, 2025) (nonprecedential).
- **Urgent concerns.** 50 U.S.C. §3033(k)(5) lets an IC employee or contractor report an "urgent concern" to the ICIG, who determines credibility and transmits it to the DNI and the intelligence committees; the employee may contact the committees directly under specified conditions. David Grusch testified that he "became a whistleblower through a PPD-19 urgent concern filing in May 2022 with the intelligence community inspector general." *Unidentified Anomalous Phenomena: Implications on National Security, Public Safety, and Government Transparency: Hearing Before the Subcomm. on National Security, the Border, and Foreign Affairs of the H. Comm. on Oversight and Accountability*, 118th Cong. 12 (July 26, 2023).

4.2 Service members

10 U.S.C. §1034 protects communications with members of Congress and IGs and lawful communications to specified persons; reprisal complaints go to the DoD IG or service IG, with relief through the Boards for Correction of Military Records.

Psychiatric referral as reprisal. Witnesses at the September 2025 House hearing described reprisal through mental-health evaluations. DoD policy forbids it: “No one may refer a Service member for an MHE as a reprisal for making or preparing a lawful communication of the type described in section 1034” (DoD Instruction 6490.04, *Mental Health Evaluations of Members of the Military Services* ¶3.e (Mar. 4, 2013, incorporating Change 1, Apr. 22, 2020)), and DoD’s military whistleblower directive lists a “[r]eferral for mental health evaluation” among the personnel actions that can be reprisal (DoD Directive 7050.06, *Military Whistleblower Protection*, Glossary (incorporating Change 1, Oct. 12, 2021)). A service member referred for evaluation after a UAP disclosure should file with the DoD IG and cite both issuances.

4.3 Civil service employees outside the IC

5 U.S.C. §2302(b)(8)-(9) protects disclosures of violations of law, gross mismanagement, and the like; for classified information, disclosures are protected only when made to an IG, OSC, or another authorized recipient. Remedies run through OSC and the MSPB (individual right of action appeal after OSC exhaustion), with review in the Federal Circuit or, for mixed cases, district court. Clearance actions themselves are outside MSPB review (*Egan*), but reprisal-based clearance actions are covered by §3341(j).

4.4 Contractor employees

- DoD, NASA, and Coast Guard contractors: 10 U.S.C. §4701 (complaint to the DoD IG; after 210 days or an adverse decision, de novo action in district court).
- Civilian-agency contractors: 41 U.S.C. §4712, which does not apply to IC elements or disclosures relating to IC activities and confers no right to disclose classified information.
- IC contractor employees: 50 U.S.C. §3234(c) (as amended, eff. Dec. 23, 2024) prohibits reprisal by agency or contractor officials against a “contractor employee” of a covered IC element for lawful disclosures to the DNI, the IC IG, agency IGs, or Congress; §3341(j) covers clearance actions.
- Department of Energy employees and contractor employees engaged in DOE defense activities (including the national laboratories that UAP allegations often name): the FY2026 NDAA moved the Atomic Energy Defense Act into title 10, and the whistleblower program formerly at 50 U.S.C. §2702 is now 10 U.S.C. §6242 (Pub. L. 119-60, §3111, 139 Stat. 1413-15). It protects disclosures “of classified or other information” that the individual reasonably believes is “direct and specific evidence” of a violation of law, gross mismanagement, or “[a] false statement to Congress on an issue of material fact,” made to a member or cleared staff of the responsible congressional committee, the DOE Inspector General, the FBI, or another designated element, if the individual “takes appropriate steps to protect the security of the information” (§6242(c)-(d)). The individual is expected to obtain the IG’s guidance before disclosing (§6242(f), (h)(3)). Reprisal complaints go to DOE’s Office of Hearings and

Appeals; the Secretary may order a contractor to abate the reprisal and sue to enforce, with “compensatory and exemplary damages” available (§6242(i)-(k)).

- §3373b(b)(2) expressly reaches reprisal by contractor officials.
- **False Claims Act retaliation.** An employee, contractor, or agent who is discharged or otherwise discriminated against for lawful acts in furtherance of an FCA action, or “other efforts to stop” FCA violations, may sue for reinstatement, double back pay, and special damages within three years after the retaliation (31 U.S.C. §3730(h)). A contractor employee who objects to UAP-related IRAD being billed as an allowable cost ([Issue D2](#)) is within it.
- **Sarbanes-Oxley.** Employees of public companies, including listed defense contractors, who report securities fraud or violations of SEC rules to a federal agency, Congress, or a supervisor are protected; the claim starts with a complaint to the Secretary of Labor, and the employee may go to federal court if there is no final decision within 180 days (18 U.S.C. §1514A(b)). A UAP program concealed in a way that made the company’s filings misleading ([Issue E4](#)) can support such a report.
- **SEC whistleblower awards.** A person who gives the SEC original information leading to a successful enforcement action with sanctions over \$1 million may receive an award, with anti-retaliation protection (15 U.S.C. §78u-6).
- **Trade secrets.** A person who discloses a trade secret “in confidence to a Federal, State, or local government official, either directly or indirectly, or to an attorney,” solely to report or investigate a suspected violation of law, is immune from liability under any federal or state trade secret law (18 U.S.C. §1833(b)). Contractor NDAs often frame program information as proprietary; the immunity answers that framing for reports to officials and counsel, though not for classified information.
- State whistleblower and wrongful-discharge law may supplement federal remedies; *Hencely v. Fluor* (2026) suggests limited preemption where the contractor’s conduct was not directed by the government ([Issue A1](#)). A court can hear such a claim even when it arises inside a special access program: in *Dubuque v. Boeing Co.*, 325 F.R.D. 296, 306-10 (E.D. Mo. 2018), *Egan* did not bar a contractor engineer’s wrongful-discharge claim over SAP debriefing procedures, because the claim did not require review of a clearance decision. The claim failed on the merits, though, because SAP manuals and NISPOM provisions were not a “clear mandate of public policy” under Missouri law, *id.* at 321. A UAP whistleblower’s state-law claim should rest on a statute, preferably §3373b(b) or 41 U.S.C. §4712, and not on security manuals alone.

4.5 Choosing a channel

Client	First channel for the disclosure	Run in parallel	Reprisal forum and first deadline	Section
IC employee or IC	Agency IG or ICIG	AARO §3373b	Agency appeal	§4.1

Client	First channel for the disclosure	Run in parallel	Reprisal forum and first deadline	Section
contractor employee	(urgent concern, 50 U.S.C. §3033(k)(5))	mechanism, for its statutory protection	within 90 days of a clearance decision (§3341(j))	
Service member	DoD IG or service IG, or a member of Congress (10 U.S.C. §1034)	AARO mechanism; PURSUE	IG complaint within one year of learning of the action (§1034(c)(5))	§4.2
Federal civilian outside the IC	Agency IG or OSC (5 U.S.C. §2302(b)(8))	AARO mechanism; PURSUE if in the Department of War	OSC, then MSPB IRA appeal within 65 days of OSC's closure letter	§4.3
DoD, NASA, or Coast Guard contractor employee	DoD IG (or NASA IG)	AARO mechanism; PURSUE	IG complaint within 3 years (10 U.S.C. §4701)	§4.4
DOE or national laboratory employee	DOE IG or a designated committee (10 U.S.C. §6242)	AARO mechanism	Under §6242	§4.4

Whatever the channel, the client should disclose nothing classified to a journalist, an author, a podcast, or an uncleared lawyer ([Issue C3](#)), and should keep a dated record of every disclosure and every adverse action.

5. Clearance risk

Clearance revocation is the most common sanction. The client should understand that:

1. A clearance determination based on the substance of security concerns is largely unreviewable in court (*Egan; Lee*).
2. A clearance action taken in reprisal for a protected disclosure is prohibited by §3341(j) and by §3373b(b)(2); the remedy is administrative.
3. Adjudicators may treat unauthorized disclosure, mental-health-related concerns, or “personal conduct” as security concerns under the Adjudicative Guidelines (SEAD 4). Clients who have described unusual experiences should be counseled about how such information

is evaluated; SEAD 4 provides that “[n]o negative inference concerning eligibility under these guidelines may be raised solely on the basis of mental health counseling” (SEAD 4, App. A ¶1(c) (June 8, 2017)), and Guideline I repeats the point: “No negative inference concerning the standards in this guideline may be raised solely on the basis of mental health counseling” (*id.* ¶27). Guideline I also lists “bizarre behaviors” among conditions that may raise a concern (*id.* ¶28(a)), which is the provision an adjudicator would apply to unusual accounts.

4. Contemporaneous records of the protected disclosure (date, channel, recipient) are the client’s best evidence of causation in a reprisal case.

Using FOIA to find out whether an unauthorized-disclosure report was made. A

whistleblower who suspects that an agency reported the whistleblower’s disclosures as unauthorized can request the intelligence oversight records directly. David Grusch did so: his September 30, 2024 FOIA request sought records submitted to the DoD Senior Intelligence Oversight Official from April 1 through December 31, 2023 concerning any “unauthorized disclosure complaint” about him or about disclosures using UAP or UFO terms, and he sued on March 2, 2026. *Grusch v. U.S. Dep’t of Defense*, No. 1:26-cv-607 (LMB/WEF) (E.D. Va.), Second Joint Status Report, ECF No. 24 (June 8, 2026). DoD released forty pages on May 18, 2026, with redactions under Exemptions 5 and 6, and the parties were conferring about remaining issues. *Id.* at 2. The released records (DoD FOIA 26-F-2486 and 26-F-2570, posted in the DoD reading room) include the November 1, 2023 reply of the Senior Intelligence Oversight Official to Representative Burchett: an Air Force intelligence oversight officer had telephoned in the summer of 2023 about “preliminary information” suggesting a possible unauthorized disclosure, then reported that “the information in question had been properly coordinated so there was no unauthorized disclosure”; no complaint was filed and the office took no action. Oversight offices keep records of preliminary reports even when no complaint is opened, and a congressional office’s inquiry made with the client’s Privacy Act release can produce a written account sooner than FOIA does.

6. The September 9, 2025 hearing and pending proposals

The House Oversight Task Force on the Declassification of Federal Secrets held a hearing titled “Restoring Public Trust Through UAP Transparency and Whistleblower Protection” on September 9, 2025, with testimony from service members and veterans who described reprisals, and from the Project On Government Oversight. The New Paradigm Institute’s draft “Enhanced UAP Whistleblower Protection Act of 2026” would amend Title 5 to create a UAP-specific reprisal remedy with a private right of action in district court, prohibit reprisal through psychiatric testing, void NDAs that bar reporting to Congress, and authorize immunity grants through 2029. It has not been introduced.

7. Counseling checklist for a prospective UAP whistleblower

1. Identify the client’s status (IC employee, DoD civilian, service member, contractor, former) and every agreement signed (SF-312, SF-4414, SAPIAs, contractor NDAs).

2. Do not take classified information from the client. Counsel without a clearance should hear only unclassified descriptions.
 3. Choose channels: §3373b (primary); PURSUE (if DoW-connected); IG/urgent concern (if alleging wrongdoing, including concealment from Congress); committees through proper channels.
 4. Obtain the written procedures for each channel and confirm the recipient is authorized.
 5. Make the disclosure; keep a dated record; request written acknowledgment.
 6. Before any public statement, submit it for prepublication review ([Form B4-1](#)).
 7. Monitor for adverse actions; file reprisal complaints promptly under the applicable statute, observing exhaustion requirements (*Akerman*).
 8. Assess criminal exposure from past conduct ([Issue C3](#)) and consider proffer or immunity ([Issue B3](#), Form B3-2) before testimony to Congress or a commission.
-