Criminal Exposure of UAP Insiders Who Disclose Information

Version 1.10 · October 2026 · nhilaw.com/issues/c3.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

- Unauthorized disclosure of classified UAP information to the press is the highest-risk act: public interest and good motive are not defenses (*Morison*; *Sterling*; *Kiriakou*).
- A disclosure through the AARO mechanism "is not a violation of section 798 of title 18, or other provision of law relating to the disclosure of information" (50 U.S.C. §3373b(b)(1)(C)); prior retention at home is not covered.
- The Atomic Energy Act's death penalty was repealed in 1969; threats that witnesses could be executed under it misstate the law.
- Sentencing levels for §793 offenses are high (U.S.S.G. §§2M3.2-2M3.3), and recent sentences run to years.
- Return any classified material through security channels before or with the disclosure, without counsel taking possession.

---

1. Summary

An insider who discloses UAP information can face prosecution under the Espionage Act and related statutes if the disclosure is unauthorized. Unauthorized disclosure to the press is the highest-risk act: the government has prosecuted it repeatedly and won (*United States v. Morison*, 844 F.2d 1057 (4th Cir. 1988); *United States v. Sterling*, 860 F.3d 233 (4th Cir. 2017)). Public interest and good motive are not defenses. Courts have declined to recognize a whistleblower defense under §793.

Since 2022 the law has given insiders a safe channel. A disclosure made through the AARO authorized reporting mechanism "is not a violation of section 798 of title 18, or other provision of law relating to the disclosure of information." 50 U.S.C. §3373b(b)(1)(C). Disclosures to inspectors general and to the intelligence committees through the statutory channels are authorized, and the Department of War's PURSUE waiver authorizes communications to PURSUE representatives. Outside those channels, the statutes below apply with full force.

Insiders also face exposure for past conduct within programs (false statements to Congress or investigators, records destruction, misuse of funds), addressed in Issue D3. And retention of classified material at home, often the first step toward a disclosure, is itself a crime.

2. Statutes

Statute	Conduct	Key elements	Maximum
18 U.S.C. §793(d)	Lawful possessor willfully communicates national defense information (NDI) to a person not entitled, or willfully retains and fails to deliver it on demand	NDI (closely held; potentially damaging); willfulness; for intangible information, reason to believe it could injure the U.S. or aid a foreign nation	10 years
18 U.S.C. §793(e)	Unauthorized possessor willfully communicates or retains NDI	Same; reaches non-government recipients	10 years
18 U.S.C. §793(f)	Gross negligence causing loss or removal of NDI	Gross negligence	10 years
18 U.S.C. §798	Knowingly and willfully communicates or publishes classified communications intelligence information	Classified COMINT; no intent-to-injure element	10 years
18 U.S.C. §1924	Officer, employee, or contractor knowingly removes classified material and retains it at an unauthorized location	Knowledge; intent to retain at unauthorized location	5 years

Statute	Conduct	Key elements	Maximum
18 U.S.C. §641	Theft or conversion of government property, including records and information (circuit split on intangible information)	Value threshold for felony	10 years
42 U.S.C. §§2274-2277	Communication of Restricted Data with intent to injure or reason to believe; disclosure by employees	Restricted Data	Up to life (§2274(a))
50 U.S.C. §3121	Disclosure of identities of covert agents	Identity of covert agent	15 years
18 U.S.C. §1001	False statements to federal investigators or Congress	Materiality	5 years
18 U.S.C. §1505, §1512	Obstruction of congressional or agency proceedings	Corrupt intent	5-20 years

The Atomic Energy Act and the "death sentence" threat. Insider accounts report that program witnesses were told the Atomic Energy Act "could be used to sentence them to death" (Jay Stratton, *Out of the Shadows* chs. 8, 36 (2026)). Congress removed the death penalty from the Act's Restricted Data offenses in 1969 (Pub. L. 91-161, §§2-3, 83 Stat. 444). The most serious offense, communicating Restricted Data "with intent to injure the United States or with intent to secure an advantage to any foreign nation," now carries a maximum of life imprisonment (42 U.S.C. §2274(a)), and communication with only "reason to believe" the data will be so used carries ten years (§2274(b)). A client who has been told otherwise should be told the actual law. A threat of that kind made to deter a witness from reporting to an inspector general or Congress may itself be witness tampering or retaliation (Issue D3).

Computer offenses. Obtaining classified information by exceeding authorized access to a government computer and willfully delivering or retaining it is a separate felony (18 U.S.C. §1030(a)(1)), often charged alongside §793.

Section 641 and intangible information. Courts long divided over whether confidential government information, as opposed to documents, is a "thing of value" under §641. The Second Circuit first held that confidential agency information about planned rate changes was a "thing of value" and "property." *United States v. Blaszczak*, 947 F.3d 19 (2d Cir. 2019). After the Supreme Court

vacated that judgment in light of *Kelly v. United States*, 590 U.S. 391 (2020), the government agreed that the information "does not constitute 'property' or a 'thing of value'" for the substantive §641 and fraud counts and confessed error, and the Second Circuit remanded for dismissal of those counts. *United States v. Blaszczak*, 56 F.4th 230 (2d Cir. 2022). The court did not rest only on the concession. It distinguished *United States v. Girard*, 601 F.2d 69, 71 (2d Cir. 1979), which held that confidential DEA records identifying informants were a "thing of value," because that kind of "inherently valuable law enforcement information" is not comparable to an agency's planned reimbursement rates. 56 F.4th at 244. District courts in the Second Circuit continue to apply *Girard* after *Kelly*: selling an agency's nonpublic records to an outsider is still a §641 offense, both because the records are "inherently valuable" and because §641 expressly reaches anyone who "sells any record of the United States." *United States v. Rodrigues*, No. 22-cr-391, 2024 WL 113744, at *4-5 (S.D.N.Y. Jan. 10, 2024) (NLRB records sold to a consultant). Information about a classified UAP program is closer to* Girard* than to *Blaszczak*: its value to the government lies in keeping it secret, and its disclosure is the harm the classification system exists to prevent. *Blaszczak* therefore gives a discloser of intangible program information an argument, but a weak one, and §641 remains a serious risk for anyone who removes or sells physical records, media, or recovered material, which are government property in the ordinary sense.

---

3. Leading cases

- **Morison** (4th Cir. 1988): a Navy analyst who gave classified satellite photographs to *Jane's Defence Weekly* was convicted under §793(d) and (e); the court rejected the argument that §793 is limited to classic espionage and held that disclosure to the press is covered.
- **Rosen** (E.D. Va. 2006): §793 reaches non-government recipients who pass NDI on; information must be closely held; for intangible information the government must show a bad-faith purpose to harm the United States or aid a foreign government; the government's closely held confirmation of public information can itself be NDI. 445 F. Supp. 2d 602 (Issue B4). The same court later refused to apply the bad-faith requirement to a trained government employee (*Kiriakou*, below).
- **Sterling** (4th Cir. 2017): a former CIA officer was convicted for disclosing classified information about a covert program to a journalist. According to the indictment and trial coverage, Sterling had raised his concerns about the program with two Senate Intelligence Committee staff members in March 2003, an authorized channel; the government used that meeting as evidence of motive, and the earlier authorized contact gave no protection for the later disclosure to a reporter. (The Fourth Circuit opinion does not discuss the meeting.) The court affirmed most counts and vacated one on venue grounds. 860 F.3d 233.
- **Schulte** (S.D.N.Y. 2021): files containing CIA work product on classified cyber tools were NDI; evidence supported transmission and retention counts, but not a count based on disclosure of a network connection the government had not shown to be closely held; false statements and obstruction convictions also supported. 578 F. Supp. 3d 596.
- **Other recent prosecutions** (outcomes as announced by the Department of Justice): *United States v. Kim*, No. 1:10-cr-225 (D.D.C.) (808 F. Supp. 2d 44, 52-57 (D.D.C. 2011) (denying

motions to dismiss: §793(d) is not vague as applied to oral disclosure of NDI by a cleared official, and the official, who had a duty not to disclose, "cannot use the First Amendment to cloak his breach of that duty")); *United States v. Drake*, No. 1:10-cr-181 (D. Md.); *United States v. Winner*, No. 1:17-cr-34 (S.D. Ga.); *United States v. Teixeira*, No. 1:23-cr-10159 (D. Mass.); *United States v. Hale*, No. 1:19-cr-59 (E.D. Va.) (drone-program documents given to a reporter; guilty plea under §793(e); sentenced July 2021). Stephen Kim, a State Department contractor, pleaded guilty in 2014 to one §793 count for giving a North Korea intelligence assessment to a Fox News reporter and received 13 months. Thomas Drake, an NSA official charged under §793(e) in 2010, saw the felony counts dropped in 2011 and pleaded to a misdemeanor of exceeding authorized use of a government computer, with probation and community service. Reality Winner, an NSA contractor, pleaded guilty under §793(e) in 2018 to giving a classified report to a news outlet and received 63 months. Jack Teixeira, an Air National Guardsman, pleaded guilty in March 2024 to six counts of willful retention and transmission of national defense information posted on a social media platform and was sentenced on November 12, 2024 to 15 years (D. Mass.). The trend is toward longer sentences and toward prosecution of retention as well as transmission.

- **Whistleblower motive.** Courts exclude or limit evidence of good motive and do not recognize a public interest defense to §793. In the prosecution of former CIA officer John Kiriakou, charged under the information clause of §793(d) for disclosures to journalists, Judge Brinkema declined to follow *Rosen*'s bad-faith gloss on the "reason to believe" element. She distinguished *Rosen* because Kiriakou was "a government employee trained in the classification system" who was "on clear notice of the illegality of his alleged communications," noted the Fourth Circuit's concern that *Rosen* imposed a burden "not mandated by the governing statute" (*United States v. Rosen*, 557 F.3d 192, 199 n.8 (4th Cir. 2009)), and held that the clause requires only that the possessor had reason to believe the information could be used to injure the United States or aid a foreign nation. Evidence that he "acted with a salutary motive, or that he acted without a subversive motive," was therefore "not relevant." *United States v. Kiriakou*, 898 F. Supp. 2d 921, 925-27 (E.D. Va. 2012) (No. 1:12-cr-127); accord *United States v. Abu-Jihaad*, 630 F.3d 102, 135-36 (2d Cir. 2010) (elements of §793(d) without intent to injure); *United States v. Diaz*, 69 M.J. 127, 132-33 (C.A.A.F. 2010). Kiriakou later pleaded guilty under the Intelligence Identities Protection Act. For a cleared insider, then, the *Rosen* bad-faith requirement is unlikely to be available in the Eastern District of Virginia; it remains arguable for a non-government recipient such as a journalist or publisher, the posture *Rosen* addressed.

3.1 Sentencing and prosecution practice

The Sentencing Guidelines set high base offense levels for these offenses: under §2M3.2 (gathering national defense information) the base level is 35 if the information was top secret and 30 otherwise, and under §2M3.3 (transmitting it) 29 and 24. Those levels explain the long sentences in *Winner* and *Teixeira*. Prosecutions remain rare compared with the number of unauthorized disclosures, which scholars attribute to the government's own selective use of leaks. David E. Pozen, *The Leaky Leviathan: Why the Government Condemns and Condones Unlawful Disclosures of*

Information, 127 Harv. L. Rev. 512 (2013). The rarity is no comfort to a client, since the cases that are brought are the ones in which the disclosure embarrassed or threatened the agency.

Classified evidence in the prosecution. In a criminal case the Classified Information Procedures Act governs: a pretrial conference (CIPA §2), a protective order (§3), government motions to delete or substitute classified discovery (§4), the defendant's mandatory notice of any classified information he expects to disclose (§5), and a hearing on its use, relevance, and admissibility, with substitutions (§6). Defense counsel must obtain a clearance early (Issue C4).

4. How §3373b changes the analysis

1. **Authorized disclosure to AARO.** §3373b(b)(1)(C) removes criminal liability under any "provision of law relating to the disclosure of information" for a disclosure through the mechanism. It also deems the disclosure compliant with EO 13526 and Atomic Energy Act rules, which should also defeat §1924 and Restricted Data theories as to the act of disclosure.
2. **Retention before disclosure.** The statute protects the disclosure itself. Prior unauthorized retention remains outside it. A client who kept classified material at home to support a disclosure remains exposed under §1924 and §793(e) for the retention. Counsel should arrange for the return of any such material through security channels before or together with the disclosure, without themselves taking possession.
3. **Onward disclosure.** A disclosure to AARO followed by a disclosure of the same information to a journalist is protected only as to the first. *Sterling* illustrates the risk.
4. **PURSUE.** The waiver addresses civil and administrative NDA enforcement only. A prosecutor would face a strong argument that a communication authorized by the Department of War was not to a person "not entitled to receive it" and was not willful, but the safer course is to use §3373b, which is statutory.
5. **Congress.** Disclosures to the intelligence committees through the ICIG urgent-concern process are authorized (50 U.S.C. §3033(k)(5)). Disclosures of classified information to individual members or staff outside that process, or to members who lack access, are not clearly authorized.
6. **A channel the site assumes is compromised.** On the site's premise that AARO is part of the concealment, the §3373b protection is still worth having, because it attaches by statute to the act of authorized disclosure. The risk is practical: AARO may share what it learns with the program the client reports on, and a later prosecutor may dispute whether a contact was made through the "mechanism for authorized reporting." Get written confirmation of the channel before the disclosure (Form C1-1).

Route	Criminal exposure	NDA / civil exposure	Clearance and employment	Reprisal remedy
AARO mechanism (§3373b)	None for the disclosure itself	None (§3373b(b)(1)(A))	Reprisal prohibited	§3373b(b)(2); IG procedures

Route	Criminal exposure	NDA / civil exposure	Clearance and employment	Reprisal remedy
PURSUE (DoW waiver)	Not addressed by the waiver; strong authorization argument	Waived for PURSUE communications	Not addressed	Existing law only
Inspector general / ICIG urgent concern	Authorized channel	Authorized	Reprisal prohibited	§3234; §3341(j); §1034; §4701
Committee through proper channels	Authorized	Authorized	Reprisal prohibited	Same
Individual member outside channels	Unclear	Possible breach	High risk	Uncertain
Journalist, podcast, social media, book without review	High (§§793(d)-(e), 798)	Breach; *Snepp* constructive trust	Revocation likely	None

5. Past program conduct

Program participants may have exposure for acts unrelated to disclosure: false statements to Congress (18 U.S.C. §1001), obstruction (§1505), destruction of records (18 U.S.C. §2071; and FY2024 NDAA §1842(a)(2)(A) for UAP records), conspiracy to defraud the United States by concealing activities from Congress (§371; *United States v. North*, 708 F. Supp. 375 (D.D.C. 1988)), and Antideficiency Act violations (administrative; criminal only if knowing and willful, 31 U.S.C. §1350). The general limitations period is five years from the offense (18 U.S.C. §3282), with no limit for capital offenses (§3281). Issue D3 analyzes these.

6. Practice guidance

1. Advise clients in writing that public or press disclosure of classified information is a crime regardless of motive and that statutory channels exist.
2. Determine whether the client holds any classified material outside authorized storage; arrange its return through the facility security officer or agency security office.
3. Use §3373b for the disclosure (Form C1-1); document authorization.

4. Before any congressional or commission testimony about program conduct, assess exposure for past acts and seek a proffer agreement or immunity (Issue B3, Form B3-2).
5. Submit any public statement for prepublication review (Form B4-1).
6. If the client is contacted by investigators, invoke counsel; consider the effect of any statement on later immunity negotiations.