OVERVIEW

Employees and contractors of the 18 elements of the U.S. Intelligence Community (IC) are excluded from protections under the Whistleblower Protection Act (i.e., the primary executive branch whistleblower law), and from non-IC federal contractor whistleblower laws. Instead, a patchwork of laws and policies dictate how IC whistleblowers may communicate protected disclosures to specific audiences. The complexity of the legal landscape is due in part to requirements around the handling of classified information. Mishandling or unlawful disclosure can lead to sanctions and criminal penalties.

INTELLIGENCE COMMUNITY

The 18 elements of the intelligence community are:

- Office of the Director of National Intelligence
- Central Intelligence Agency
- Defense Intelligence Agency
- National Security Agency
- National Geospatial Intelligence Agency
- National Reconnaissance Office
- Federal Bureau of Investigation
- The intelligence elements of the Army, Navy, Coast Guard, Marine Corps, Air Force, and Space Force
- Department of Energy’s Office of Intelligence and Counterintelligence
- Department of Homeland Security’s Office of Intelligence and Analysis
- Drug Enforcement Administration’s Office of National Security Intelligence
- Department of State’s Bureau of Intelligence and Research
- Department of the Treasury’s Office of Intelligence and Analysis

Note that while the Federal Bureau of Investigation (FBI) is an element of the IC, FBI employees are covered under a unique law discussed below. Similarly, uniformed service members working within the military intelligence elements fall under the Military Whistleblower Protection Act.

Classified Information

While not all disclosures from IC whistleblowers involve classified information, classified disclosures can only be made through secure channels and between those with proper access. Members of Congress may generally access classified information without a security clearance by nature of their position, but congressional staff must have the appropriate clearance.

As a co-equal branch of government, Congress takes the position that it can lawfully receive classified disclosures that are communicated through the proper channels. Still, executive branch interpretation of whistleblower laws and policies do not always align with Congress’ stance. As such, there is a heightened risk that whistleblowers could experience adverse employment, security clearance, or legal actions.

Whistleblower Protection Act

5 U.S.C § 2302(b)(8)(C)(ii) protects disclosures of classified information to Congress by employees covered under the Whistleblower Protection Act. However, the information must have been classified by the head of a non-intelligence agency, and the disclosure cannot reveal intelligence sources and methods.

Legal Disclaimer: This document is for general informational purposes only. Its contents are not legal advice.
Protected Disclosures And Conduct

The Intelligence Authorization Act for Fiscal Year 2014, as amended, (50 U.S.C. § 3234), prohibits retaliation against covered employees who make a lawful disclosure of information to a protected audience. The employee must reasonably believe they are disclosing:

- A violation of any federal law, rule, or regulation
- Mismanagement
- A gross waste of funds
- An abuse of authority
- A substantial and specific danger to public health or safety

Protected audiences include:

- The Director of National Intelligence (DNI) or their designee
- The Inspector General of the Intelligence Community (ICIG)
- A supervisor in the whistleblower’s direct chain of command
- A supervisor in the relevant agency with responsibility for the subject matter of the disclosure, up to and including the head of the agency or their designee
- The inspector general (IG) of the relevant agency
- A congressional intelligence committee or any member of those committees

The law also prohibits retaliation because of certain conduct, including:

- The exercise of any appeal, complaint, or grievance right
- Testimony for, or lawfully assisting any individual with, their own appeal, complaint, or grievance right
- Cooperation with, or disclosures made to, an inspector general (IG) in connection with the IG’s audit, inspection, or investigation

Disclosing An Urgent Concern

Covered employees may also disclose matters of "urgent concern" to the congressional intelligence committees through the ICIG or their agency’s IG. The IG evaluates the credibility of the disclosure and determines whether it qualifies as an urgent concern under the statutory definition. If the disclosure passes those tests, the IG sends it to the relevant agency head who must transmit the disclosure to the congressional intelligence committees within seven days.

If the IG fails to transmit the disclosure to the agency head, the whistleblower can send their disclosure to the intelligence committees, directly. However, they must inform the IG that they are doing so and must receive and follow related instructions.

Urgent Concern Defined

The law defines an urgent concern as:

- A serious or flagrant problem, abuse, violation of law or executive order, or deficiency relating to the funding, administration, or operation of an intelligence activity that is a matter of national security and not a difference of opinion concerning public policy matters;
- A false statement to Congress, or a willful withholding from Congress, on an issue of material fact relating to the funding, administration, or operation of an intelligence activity; or
- An action, including a personnel action described in section 2302(a)(2)(A) of Title 5 constituting reprisal or threat of reprisal prohibited under section 7(c) in response to an employee’s reporting an urgent concern in accordance with this section.


WHISTLEBLOWER RETALIATION

50 U.S.C. § 3234 prohibits retaliation in response to protected whistleblowing, protected conduct, and urgent concern disclosures. The law does not explicitly dictate procedures for enforcement, but instead requires the president to provide enforcement mechanisms in line with those Congress developed under the Whistleblower Protection Act. Executive branch policies are laid out in Presidential Policy Directive-19 (PPD-19), Intelligence Community Directive-120 (ICD-120), and in agency policies.

Administrative Enforcement Process

Sections A and C of PPD-19 lay out general rights for relief from whistleblower retaliation, beginning with a retaliation complaint to the relevant office of inspector general. ICD-120 further expands on these sections for applicability to the IC elements.
Under PPD-19 Section A, an inspector general conducts an investigation into the whistleblower’s complaint and issues a report with their findings and recommendations for corrective action. The IG’s report is not binding; the relevant agency head reviews it and then makes the final decisions regarding corrective action.

PPD-19 Section C provides an appeal process. The whistleblower can seek to overturn an unfavorable initial decision by requesting an external review panel made up of three IGs, including the ICIG. If convened, the panel has six months to investigate the whistleblower’s retaliation claim and issue a new report. The agency head then re-considers their initial decision, under advisement of the panel’s findings. Note that while IC contractors are protected from whistleblower retaliation by law, PPD-19’s coverage of these individuals has been limited to Part B which only deals with security clearance actions.

To succeed, whistleblowers must demonstrate that their lawful whistleblowing was a “contributing factor” in the clearance or access decision. If they meet that standard, the defending agency must demonstrate by a “preponderance of the evidence” that the clearance action was legitimate. A whistleblower may appeal their case to the Director of National Intelligence within 60 days.

SECURITY CLEARANCE RETALIATION

The Intelligence Reform and Terrorism Prevention Act (50 U.S.C. § 3341(j)), prohibits taking, failing to take, or threatening to take any action with respect to a covered employee’s security clearance, or their access to classified information, in retaliation for the employee’s lawful whistleblowing. The law protects federal employees of executive agencies, including the FBI and other IC elements; military service members; and employees of federal contractors, subcontractors, grantees, subgrantees, and personal services contractors. PPD-19 Part B and ICD-120 Section F also cover retaliatory security clearance actions, and the PPD-19 Part C appeals process, as described above, is available to challenge an unfavorable initial decision.

FBI EMPLOYEE WHISTLEBLOWING

Federal employees of the Federal Bureau of Investigation (FBI) are covered under the FBI Whistleblower Protection Enhancement Act (5 U.S.C. § 2303). Note that FBI contractors are covered under 50 U.S.C. § 3234, discussed above. Under the Act, FBI employees may disclose misconduct that they reasonably believe evidences:

- A violation of any Federal law, rule, or regulation
- Gross mismanagement
- A gross waste of funds
- An abuse of authority
- A substantial and specific danger to public health or safety

Protected audiences include:

- The employee's chain of command
- The Justice Department Office of Inspector General
- Congress
- The Office of Special Counsel
- The Offices of Professional Responsibility of the Justice Department and FBI
- The FBI Inspection Division

FBI employees may file a retaliation complaint with either the Justice Department Office of Inspector General or the Office of Professional Responsibility pursuant to FBI whistleblower regulations (28 C.F.R. part 27). FBI employees may appeal an unfavorable or delayed agency determination to the Merit Systems Protection Board pursuant to 5 U.S.C. § 1221.

Administrative Enforcement Process

Enforcement is administrative and begins with a filing to the agency OIG within 90 days. Notably, a clearance suspension must be for at least one year to be challenged as retaliatory.

ADDITIONAL RESOURCES

Congressional Research Service: Intelligence Community Whistleblower Provisions
Executive Order 12968: Access to Classified Information
Intelligence Community Directive 120: Intelligence Community Whistleblower Protections
Office of the Director of National Intelligence: Introducing IC Whistleblowing