ICW&SP Fact Sheet (Rev. C, March 12, 2014)

Statutes and guidelines currently exist to protect American intelligence community whistleblowers

Dan Meyer, Executive Director of Intelligence Community Whistleblowing & Source Protection
Office of the Inspector General of the Intelligence Community

The Intelligence Community Whistleblowing & Source Protection directorate (ICW&SP)[1] supports the Intelligence Community Inspector General (IC IG) Forum[2] by assisting members of the Forum with the administration of programs designed to promote whistleblowing as an internal function, and to protect the employees, contractors, and other sources of information that contribute to IG investigations, audits, evaluations and reviews of fraud, waste, and abuse.

Concept of Operations. Whistleblower — or source protection — in the intelligence community is not the same as protection of an employee's or contractor's civil liberties or First Amendment rights to speech and assembly. Rather, whistleblower protection seeks to protect sources reporting internal corruption, the same corruption all Federal employees have been required to report under Executive Order 12674 since 1991.[3] Much of this reporting involves simple Executive Branch management issues (time and attendance fraud, workplace violence, etc.). But the disclosures receiving the most attention, however, are usually those which trigger Constitutional concerns under the Separation of Powers doctrine, including the sub-doctrine of Executive Privilege. At the core of the process is the sovereign's "need to know" as that need is satisfied through the normal working relations between the Legislative and Executive branches.[4]

---

[1] ICW&SP operations are divided into three categories: (1) Disclosures & Appeals (including de novo investigations); (2) Outreach to promote whistleblowing; (3) Training to increase the effectiveness of the response to allegations of reprisal against whistleblowers. ICW&SP went "operational" with respect to outreach on September 15, 2013. The first IC-wide investigative training occurred at a leadership level on December 17, 2013 and the first dedicated training of investigators occurred the next month, on January 15, 2014. The first disclosures to Congress were processed in January 2014; the first appeals were received in February 2014. ICW&SP's plan of operations is based on work done in this area by the Department of Defense Inspector General, and the inspectors general of the National Security Agency and the Defense Intelligence Agency between 2004 and 2010.

[2] The IC IG Forum serves as a mechanism for informing its members of the work of individual members of the Forum that may be of common interest as well as sharing information, best practices, and assisting with access to employees, employees of contract personnel, records, audits, reviews, documents, recommendations, or other materials that may involve or be of assistance to more than one of the member IGs. See. 50 U.S.C. § 3033(h)(2).

[3] Para. (k), Executive Order 12674 of April 12, 1989 (as modified by E.O. 12731).

[4] There are three other important areas of law which occasionally overlap with the whistleblower protection laws. First, if a whistleblower seeks information to prove that he/she has suffered retaliation, Executive branch officials may deny the request under an application of the Privacy Act and Freedom of Information Act, which has an unintended or perhaps intended consequence of shielding management from embarrassment. Over application of these statutes can also have the perverse effect of denying the public examples of their government officials acting appropriately to protect whistleblowers and discipline management officials for engaging in reprisals after a whistleblowing incident. Second, the laws and regulations governing the detection and assessment of Insider Threats can lead to unauthorized disclosure investigations designed to curtail the release of information to the Congress. Third, given the centrality of Agency law departments to the legal sufficiency review of whistleblower reprisal reports of investigation, the decentralized nature of Federal attorney professional responsibility and regulation can lead to an imbalance in the relations between client and attorney as whistleblower investigations unfold.

Accordingly, the promotion of whistleblowing *as an accepted Federal mission* to be participated in by all supervisors, managers and employees empowers the Federal bureaucracy in the fight against the domestic, internal corruption which can undo the excellent work done by our Armed Services and Intelligence community operators safeguard the Republic against foreign enemies.

It is important to understand whether the word "whistleblower" is being used in the vernacular or legal sense. For the purposes of conducting investigations, *whistleblower* is a legal term of art. It relates to *lawful* disclosures. It refers to a specific process for bringing certain classified and unclassified matters to the attention of those who may correct the wrongdoing. *Whistleblowing* does not included policy disputes over programs/activities. In contrast, *unlawful* communications are not whistleblowing, they are "leaks" in the vernacular and may subject the leaker to criminal prosecutions, civil penalties, and administrative disciplinary actions.

An IC employee or contractor may make a lawful disclosure through a variety of venues. IG Hotlines or personal meetings with IG officials affords the whistleblower with statutory protection from reprisal for making such disclosures under the Inspector General Act of 1978, and similar statutes in Title 50. Similarly, certain other compliance offices have the authority/responsibility to receive certain disclosures, like violations of equal employment laws or civil liberties and privacy laws. For example, the ODNI's Civil Liberties and Privacy Office (CLPO) has the responsibility to investigate privacy and civil liberties complaints within ODNI, and to refer complaints relating to other IC elements to their IGs.

Statutory and Policy Protections for IC Whistleblowers. The following statutory and policy protections provide protections for IC Whistleblowers:

(1) The Inspector General Act of 1978, as amended, allows Department of Defense Intelligence Community employees to report allegations of violation of laws, rules, or regulations, or mismanagement, gross waste of funds, abuse of authority, or a substantial and specific danger to the public health and safety to their respective IC element IG or the Department of Defense IG.[5]

(2) For employees of the Central Intelligence Agency (CIA), the CIA Inspector General can accept disclosures, complaints, or information from any person concerning the existence of an activity within the CIA constituting a violation of laws, rules, or regulations, or mismanagement, gross waste of funds, abuse of authority, or a substantial and specific danger to the public health and safety. [6]

(3) The National Security Act of 1947,[7] as amended, allows the IC IG to receive disclosures complaints, or information from any person concerning the existence of an activity within the authorities and responsibilities of the Director of National intelligence constituting a violation of laws, rules, or regulations, or mismanagement, gross waste of funds, abuse of authority, or a substantial and specific danger to the public health and safety. Further, this

[5] *See* The Inspector General's Act of 1978 § 8G; 5 U.S.C. App. 8G. This includes each Inspector General for the Defense Intelligence Agency (DIA), the National Geospatial-Intelligence Agency (NGA), the National Reconnaissance Office (NRO), and the National Security Agency (NSA).
[6] *See* 50 U.S.C. 3517 (e)(3).
[7] *See* 50 U.S.C. 3033 (g)(3).

statute prohibits reprisal actions taken against employees making such disclosures to the IC IG, who may investigate any reprisal allegation in addition to the initial disclosure that the employee made.

(4) The IC IG Forum Members may also receive complaints from IC employees and contractors who wish to report "urgent concerns" to Congress. This allows whistleblowers with an avenue to report classified complaints to the congressional intelligence committees for action. Again, these law disclosures are protected and reprisal actions stemming from such disclosures are prohibited.[8]

(5) The Federal Acquisition Streamlining Act of 1994 (PL 103-355), as implemented by the Federal Acquisition Regulations (FAR), provides whistleblower protection to contractor employees for "... all Government contracts ..." (FAR, subpart 3.9, Whistleblower Protections for Contractor Employees and FAR 3.902, Applicability). In general, IGs may receive reprisal complaints "relating to a substantial violation of law related to a contract (including the competition for or negotiation of a contract)." Note that the sole basis for protection is far more limited than the basis for reprisal protection under the National Security Act above, as this protective statute is available to IC contractors who disclose matters related and limited to only the contract under which they are working.[9] However, the IC IG may receive complaints from "any person," not just IC employees; regarding any violation of law, not just those violations relating to the contract. The IC IG statute prohibits reprisal actions against anyone making such disclosures to the IC IG, which allows for another more broadly scoped reprisal protection for IC contractors. See 50 U.S.C. 3033 (g)(3). The Federal Acquisitions Regulation was amended in September 2013, stating that the regulation's whistleblower protections no longer implemented the FASA provisions in 10 USC 2409 (affecting DoD, NASA and the Coast Guard). These protections were to be implemented in the FAR supplements issues by those agencies (e.g., at DoD the DFARS).[10]

---

[8] *See* Inspector General's Act of 1978 § 8H, 5 U.S.C. App. 8H;, which is commonly referred to as the Intelligence Community Whistleblower Protection Act of 1998 (ICWPA) and covers DIA, NGA, NRO, and NSA employees and contractors. The Central Intelligence Agency Act of 1949, 50 U.S.C. 3517(d)(5)(A) covers CIA employees and contractors). The IC IG statute, 50 U.S.C. 3033 (k)(5)(A), is mirrored after the ICWPA. The ICWPA which does not provide intelligence community whistleblower protection, would probably have been better entitled, "the protection of disclosures to the Congress Act". For employees disclosing to the Congressional intelligence committees under these Acts, protection is provided under the broader whistleblower protection provisions outlined in the respective IG acts stated above.

[9] At present, there is a whistleblower protection pilot program as mandated by section 828, entitled "Pilot Program for Enhancement of Contractor Employee Whistleblower Protections," of the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2013 (Pub. L. 112-239, enacted January 2, 2013). Paragraph (a) of section 828 adds to title 41 a new section 4712 that contains the elements of the pilot program, which is in effect through January 1, 2017. Under the pilot program, and under 10 U.S.C. 2409, another whistleblower protection program, these protections exclude IC contractor employees.

[10] http://spa.columbia.edu/files_sponsoredprojects/imce_shared/Whistleblower_FAR_3_908__00193229x9672E_.pdf ("FAR 3.900 Scope of subpart. This subpart implements three different statutory whistleblower programs. This subpart does not implement 10 U.S.C. 2409, which is applicable only to DoD, NASA, and the Coast Guard.").

(6) Presidential Policy Directive No. 19 (PPD-19) ensures that IC employees and individuals eligible for access to classified information can effectively report fraud, waste, and abuse while protecting classified information without fear of retaliation for making such reports. This protection allows employees to make protected disclosures, regardless of category, to management officials, agency directors, and agency Inspectors General (IG). PPD-19 prohibits reprisal actions in the form of personnel actions (Section A) or security clearance decisions (Section B) against IC employees who make such disclosures, which establishes an overarching system of IC whistleblower protection through an executive order. [11] Further, PPD-19 requires an IG review of any reprisal allegation that violates PPD-19. Initial IG reviews are completed by Agency IGs, who are also members of the IC IG Forum. If an employee has exhausted their agency review process, to include the IG review process, then he/she may appeal to the External Review Panel (ERP) led by the IC IG for an appellate review. Hearing of an appeal, or a de novo investigation in response to an appeal, is discretionary on the part of the IC IG. For IC Contractors, reprisal protections are granted under Section B of PPD-19 only, for the limited purposes of reviewing alleged reprisal through security clearance decision-making. Prior to, and in response to, PPD-19, IC elements maintained local whistleblower protection regulations, which are now certified under the PPD-19 process. [12]

Accordingly, this patchwork of statutory and policy protections creates a system dependent on the skills, talents and authorities of the many inspectors general providing oversight to the Intelligence Community. These inspectors general may make findings and recommend corrective action. But they cannot order corrective action. In order for a wronged whistleblower to receive a remedy or for a wrongful responsible management official to be disciplined, the Agency head (or her designee) who has personnel authority over both whistleblower and reprisor must take action.

The President's decision to incorporate title 5 by reference in PPD-19 permits use of title 5's case law in the conduct of whistleblower reprisal investigations. Accordingly, this allows for use of critical doctrines such those of "perceived whistleblowers," "constructive knowledge," and the three-part test for whether the agency would have taken the action absent the disclosure. The critical distinction to understand when assisting IC whistleblowers is that unlike non-IC whistleblowers, the status of the employee or contractor is not the lead detriment in how to apply the law. Once you know you have an IC employee or contractor, it is really the venue of the disclosure, which the Legislature and the Executive Branch have made the most important metric in classifying the case.[13]

---

[11] Since 1982, sources to Defense Intelligence Community intelligence oversight (I/O) investigations and reviews have had protection under Procedures 14 & 15 of the regulations implementing the Foreign Intelligence Surveillance Act of 1978, as amended. The term "employees" under this Act has been read to include contractors since at least 2004. These investigations would probably now be routed through the Department of Defense Office of the Inspector General, and reviewed under the provisions of PPD-19.

[12] Several IC elements already had whistleblower policies that provided reprisal protections for IC employees and contractors. PPD-19 enhanced those existing policies by creating a uniform prohibition on reprisal actions for making protected disclosures as well as requiring an IG review of reprisal allegations.

[13] There has been a fair amount of confusion regarding the protection of IC contractors. Given the limits of the laws provided, IC contractors (and those disclosing on FISA matters in particular) have had substantially the same protections as non-contractors since 1982. "Existence" of the protections really can not be debated; "effectiveness" is always a useful issue to review.

Protected Disclosures. Making a disclosure is the first step in gaining protection. Individuals within the IC, whether they are government employees or contractors, can make reports of fraud, waste, abuse, and violations of law through their management chains, all the way up to the head of an IC element, and to their respective IG.

If an IC employee wishes to report an "urgent concern" to the Congress, he or she may do so through either the IC element's IG or through the IC IG under the ICWPA and related statutes as mentioned above. These reports to the IG are also "protected disclosures," which means that employees and contractors are protected from reprisal actions for making such disclosures. Moreover, the IGs have a responsibility to report directly to Congress any instances of management officials refusing to cooperate with an IG review of such a matter that has been reported to the IGs. These provisions ensure that IC employees and contractors have a protected avenue to make reports of alleged wrongdoing to Congress without compromising sensitive and classified information or fearing retaliation actions.[14]

In addition to ICWPA and disclosures to statutory inspectors general, employees and contractors making disclosures of questionable activities under the Intelligence Oversight regulations (such as Department of Defense Procedures 14 & 15) also qualify as having made a "protected disclosure".

PPD-19 Policies and Processes.[15] Once a protected disclosure is made, PPD-19 provides an avenue to protect the whistleblower making the disclosure. PPD-19 requires each IC agency to establish:

(1) policies and procedures prohibiting retaliation against employees who make protected disclosures,

— and —

(2) policies and procedures for these claims to be reviewed by the agency's IG , who will make a recommendation to the agency head on appropriate relief if retaliation is proven.

To the fullest extent possible, PPD-19 requires these IC agency policies and procedures to mirror those of the Whistleblower Protection Act (5 U.S.C. § 2302(b)(8)). The requirements of PPD-19 are currently being implemented.

If an employee has exhausted his or her remedies under the agency process, he or she may seek review by the External Review Panel (ERP), a panel of three Inspectors General chaired by the IC IG. The IC IG may make a recommendation to the agency head for appropriate action or may exercise de novo investigative jurisdiction over the matter appealed.[16]

Structurally, PPD-19 is divided into two core functional parts: Section A (providing whistleblower protection for IC community members) and Section B (providing whistleblower protection for all Federal security clearance applicants and holders). The standards for assessing reprisal under Section A are provided by the President's citation to title 5 of the United States Code. In contrast, Section B cites

---

[14] See Inspector General's Act of 1978 § 8H, 5 U.S.C. App. 8H; Central Intelligence Agency Act of 1949 § 17(d)(5) (for CIA employees and contractors); National Security Act of 1947 § 103H(k)(5)(A) (for the Intelligence Community at large)).

[15] PPD-19 generally does not apply to the FBI, which follows a different statutory regime. For the text of the President's directive, PPD-19, part A, *go to* http://www.whitehouse.gov/sites/default/files/image/ppd-19.pdf

[16] PPD-19, Section C.

simply to Executive Order 12968, Access to Classified Information (Aug. 4, 1995), which does not have a whistleblower protection clause providing standards. Because PPD-19 does not have a standard by which an IG investigator can conduct an investigation, the IC IG applies title 5 standards identical to those cited by the President in Section A through E.O. 12968, for all PPD-19 investigations for both Section A and Section B. These standards are outlined in Section 3.1, and require eligibility and access to be "clearly consistent with the interests of national security." See E.O. 12968, Sec. 3.1. (b)&(d).[17]

Access to Classified Information (Security Clearances). PPD-19 also prohibits agencies from taking an action to revoke or deny an employee's eligibility for access to classified information (i.e., the employee's security clearance) in retaliation for making a protected disclosure. The relevant executive orders implementing the eligibility system (E.O. 12968 for government employees) already include due process procedures for suspension and revocation of access to classified information. In addition to these due process procedures, PPD-19 requires all agencies to develop a review process that allows employees to appeal an action affecting eligibility for access to classified information if they allege that such action was made in retaliation for making a protected disclosure. As part of this additional review process, PPD-19 also requires a review by the agency's Inspector General to determine whether PPD-19 has been violated and if so, to make recommendations for the agency to reconsider the employee's access to classified information. Employees who claim retaliation due to actions affecting security clearances may also take advantage of the external IG panel review discussed above.[18]

Intelligence Community contractors. Contractors are not covered by the Whistleblower Protection Act, or Part A of PPD-19. However, the Intelligence Community Whistleblower Protection Act applies to IC contractors, providing contractors with a protected avenue to make reports of urgent concern to congressional committees without compromising sensitive and classified information.

Executive Order 10865, which establishes the Industrial Security Clearance Program, includes the due process requirements for the revocation of access to classified information for contractors, including providing the contractors with the right to a due process hearing. Part B of PPD-19 may also provide additional protections for contractors who claim retaliation. The Executive Branch is evaluating the scope of that protection as we implement the requirements of the PPD. Presidential Policy Directive 19 (PPD-19) is currently in its implementation phase. Agencies are required to certify their compliance with the PPD to the DNI, who will review the certifications and inform the President of compliance.

---

[17] For example, reporting of corruption within the federal Government is required by E.O. 12674. Where there are allegations that the national security interest has been compromised by reprisal against a source, we apply title 5 standards to ascertain whether those reporting corruption are being reprised against for their reporting.

[18] PPD-19, Section B.