Congressional Research Service
Informing the legislative debate since 1914

# Intelligence Whistleblower Protections: In Brief

**name redacted**
Legislative Attorney

October 23, 2014

**Congressional Research Service**
7-....
www.crs.gov
R43765

**CRS REPORT**
Prepared for Members and
Committees of Congress

# Summary

Intelligence whistleblowers are generally Intelligence Community (IC) employees or contractors who bring to light allegations of agency wrongdoings by, for example, disclosing information on such wrongdoings to congressional intelligence committees. Such disclosures can aid oversight of, or help curb misconduct within, intelligence agencies. However, intelligence whistleblowers could face retaliation from their employers for their disclosures, and the fear of such retaliation may deter whistleblowing. Congress and President Obama have taken measures to protect certain intelligence whistleblowers from retaliation, and thereby seemingly encourage these whistleblowers to disclose information on agency wrongdoing. These measures are the Intelligence Community Whistleblower Protection Act of 1998 (ICWPA), Presidential Policy Directive 19 (PPD-19), and Title VI of the Intelligence Authorization Act of 2014 (Title VI). Each of these measures details what disclosures fall within the scope of its protections, which generally include certain disclosures through government channels (e.g., disclosures to agency inspectors general or congressional intelligence committees). None of these measures protect against retaliation or potential criminal liability arising from disclosures to media sources. The ICWPA applies to both IC employees and contractors, whereas PPD-19 and Title VI appear to apply only to IC employees.

The ICWPA is the oldest of the three intelligence whistleblower protections and, of the three, provides the least amount of protection to those falling within its scope. The ICWPA does not explicitly prohibit retaliation against IC whistleblowers. Rather, it outlines procedures through which whistleblowers can disclose to the congressional intelligence committees information on "urgent concerns," such as violations of law or false statements to Congress. The ICWPA further contains no explicit mechanism for obtaining a remedy for retaliation stemming from disclosure of an urgent concern to Congress. It merely allows an IC whistleblower who has faced an adverse personnel action because he disclosed an urgent concern to the congressional intelligence committees to then use the ICWPA's disclosure procedures to inform the committees of the retaliation.

PPD-19, unlike the ICWPA, expressly prohibits an IC employee from taking an adverse personnel action or security clearance determination against another employee because of a protected disclosure. It additionally requires intelligence agencies to develop procedures for internally investigating, through agency Inspectors General, allegations of impermissible retaliation. After finding that impermissible retaliation has occurred, Inspectors General can recommend that agency heads take corrective action. When an employee has exhausted the internal review procedures that must be established under PPD-19, he can appeal to the Director of National Intelligence, who then has the discretion to convene a review panel. If it finds that improper retaliation occurred, the review panel can recommend that the agency head take remedial action.

Title VI seemingly codifies, and expands upon, some of the protections of PPD-19. Its protections, and modes of enforcement, differ depending on the type of retaliation alleged. More specifically, Title VI's protected disclosures and enforcement methods in the context of allegations of adverse personnel action are distinct from its protected disclosures and enforcement methods for allegations of adverse security clearance or information access determinations.

# Contents



## Contacts

# Introduction

Generally speaking, whistleblowers are those who expose misconduct (e.g., fraud, abuse, or illegal activity) within an organization. In the context of the Intelligence Community (IC), whistleblowers are generally employees or contractors of federal intelligence agencies who bring to light information on agency wrongdoings. Whistleblowers disclose this information through government channels (e.g., the congressional intelligence committees or agency inspectors general) or to the media. Such disclosures can aid oversight of, and thereby curb misconduct within, intelligence agencies. When an IC whistleblower discloses information on alleged agency wrongdoing, he could face retaliation from his employer by, for example, being fired, demoted, or having his security clearance revoked.

The threat of retaliation may deter potential whistleblowers from disclosing information on agency wrongdoing. There is seemingly tension between the desire to eliminate this deterrence, and thus encourage whistleblowers to bring agency misconduct to light, and the need to protect government secrets which, if disclosed publicly, could be harmful to the country's national security interests. Apparently seeking to strike balance within this tension, Congress and President Obama have taken action to limit retaliation against IC whistleblowers for certain types of protected disclosures, which do not include disclosures to media sources. That is, IC whistleblowers who disclose information to media sources generally are unprotected against potential retaliation or criminal sanction.

There are three sources of protections against retaliation for IC whistleblowers: the Intelligence Community Whistleblower Protection Act of 1998 (ICWPA),[1] Presidential Policy Directive 19 (PPD-19),[2] and Title VI of the Intelligence Authorization Act for Fiscal Year 2014 (Title VI).[3] Before passing the ICWPA, which is the oldest of the three protections, Congress observed that intelligence whistleblowers apparently lacked protection against retaliation stemming from their disclosures of agency wrongdoings.[4] Whistleblower protections for federal employees are largely governed by the Whistleblower Protection Act (WPA), which Congress initially passed in 1989, and its amendments.[5] The WPA expressly excluded intelligence agency employees from its applicability, and thus initially left intelligence whistleblowers unprotected against retaliation.[6] The ICWPA seemingly represented Congress's attempt at filling this gap by extending protections to intelligence whistleblowers.

Though the ICWPA extended some protections to intelligence whistleblowers, it afforded such whistleblowers less protection than the WPA affords non-intelligence whistleblowers. However, protections for intelligence whistleblowers have strengthened over time. PPD-19, which President

[1] P.L. 105-272, 112 Stat. 2396 (1998).

[2] OFFICE OF THE WHITE HOUSE PRESS SECRETARY, PRESIDENTIAL POLICY DIRECTIVE 19- PROTECTING WHISTLEBLOWERS WITH ACCESS TO CLASSIFIED INFORMATION (Oct. 10, 2012), hereinafter PPD-19.

[3] P.L. 113-126, 128 Stat. 1390, 1414 (2014).

[4] *See* S.Rept. 105-165, at 2 (1998).

[5] P.L. 101-12, 103 Stat. 16 (1989).

[6] The WPA, by its text, does not apply to employees of "the Federal Bureau of Investigation, the Central Intelligence Agency, the Defense Intelligence Agency, the National Geospatial-Intelligence Agency, the National Security Agency, the Office of the Director of National Intelligence, and the National Reconnaissance Office." 5 U.S.C. §2302(a)(2)(C).

Obama issued in 2012, expanded upon the ICWPA's protections for some IC whistleblowers, and Title VI generally codified, and in some instances built upon, the protections of PPD-19. This report describes these three sources of IC whistleblower protection.

# Intelligence Community Whistleblower Protection Act of 1998

The ICWPA is the oldest of the three intelligence whistleblower protections. In passing the ICWPA, Congress observed that the threat of adverse personnel action to IC employees deterred them from whistleblowing.[7] This deterrence from whistleblowing, Congress found, may have been constricting the flow of information to congressional intelligence committees that the committees needed to properly perform their oversight responsibilities.[8] The ICWPA therefore permits IC employees and contractors to bring a complaint or disclose specified information to Congress, and outlines the procedures for doing so. However, the ICWPA does not expressly prohibit retaliation against IC whistleblowers for permissibly bringing a complaint or information to Congress and contains no explicit mechanism for obtaining a remedy for this retaliation. Rather, the ICWPA merely allows an IC whistleblower who has faced such retaliation to then use the act's disclosure procedures to inform the intelligence committees that the retaliation has occurred.

The ICWPA applies to employees of the Central Intelligence Agency, Defense Intelligence Agency, National Imagery and Mapping Agency, National Reconnaissance Office, National Security Agency, Federal Bureau of Investigation, and any other agency that the President determines has the principal function of conducting foreign intelligence or counterintelligence activities.[9] The ICWPA also applies to the employees of a contractor of any of the aforementioned agencies.[10] An employee seeking to bring a complaint or disclose information to Congress under the ICWPA is subject to two limitations: (1) the complaint or information must be related to an "urgent concern" as defined in the act; and (2) the employee must first bring the complaint or disclose the information to the agency head through the proper agency channels.

Under the ICWPA, IC employees and contractors can disclose to Congress only complaints and information that are "with respect to an urgent concern."[11] Under the act, an "urgent concern" can be one of three things.[12] First, it can be a "serious or flagrant" abuse, problem, violation of executive order or law, or deficiency in funding, agency administration, or agency operations involving classified information.[13] Second, an urgent concern can be a false statement to, or

[7] *See* P.L. 105-272, §701-02, 112 Stat. 2396, 2413 (1998).

[8] *Id.*

[9] The ICPWA provisions relating to employees and contractors of the Central Intelligence Agency (CIA) are at 50 U.S.C. §3517(d)(5). The parallel ICPWA provisions relating to employees and contractors of the Defense Intelligence Agency, National Imagery and Mapping Agency, National Reconnaissance Office, National Security Agency, Federal Bureau of Investigation, and any other agency that the President determines has the principal function of conducting foreign intelligence or counterintelligence activities are at 5 U.S.C. app. §8H.

[10] 50 U.S.C. §3517(d)(5)(A); 5 U.S.C. app. §8H(a)(1)(A), (B).

[11] 50 U.S.C. §3517(d)(5)(A); 5 U.S.C. app. §8H(a)(1)(A), (B).

[12] 50 U.S.C. §3517(d)(5)(g); 5 U.S.C. app. §8H(h)(1).

[13] 50 U.S.C. §3517(d)(5)(g)(i)(I); 5 U.S.C. app. §8H(h)(1)(A). It cannot, however, be a difference in opinion on public policy matters. 50 U.S.C. §3517(d)(5)(g)(i)(I); 5 U.S.C. app. §8H(h)(1)(A)

willful withholding from, Congress on an issue of material fact relating to intelligence activity funding, administration, or operation.[14] Third, an urgent concern can include adverse personnel action stemming from disclosure under the ICWPA.[15] A complaint or information that is not regarding one of these three "urgent concerns" is not covered by the ICWPA.[16]

IC employees and contractors must first bring complaints or information regarding "urgent concerns" to the agency head through proper agency channels, as described in the ICWPA, before bringing them to Congress. This generally requires first bringing a complaint or information to the agency's Inspector General or the Inspector General of the IC (IGIC),[17] who then has 14 calendar days to evaluate the credibility of the complaint or information.[18] Upon finding the complaint or information credible, the Inspector General must send notice of its finding, along with the complaint or information, to the agency head within the 14-calendar-day period for evaluation.[19] The agency head then has 7 calendar days from receipt of the Inspector General's notice to forward the notice, along with any of the agency head's comments, to the congressional intelligence committees.[20]

The ICWPA allows employees to contact intelligence committees directly if the Inspector General either does not find the complaint or information credible, or sends the agency head an inaccurate complaint or inaccurate information.[21] However, this ability to contact the intelligence committees directly is subject to two limitations. First, before making such contact, an employee or contractor must give the agency head a statement of the complaint or information through the Inspector General, along with notice of intent to contact the intelligence committees directly.[22] Second, the employee or contractor must follow the agency head's direction, given through the Inspector General, on compliance with appropriate security practices when contacting the intelligence committees.[23]

The ICWPA seemingly represents an attempt by Congress to fill a gap in federal whistleblower protections by extending such protections to IC whistleblowers where they were expressly excluded from the WPA and its amendments, which generally provide whistleblower protections

[14] 50 U.S.C. §3517(d)(5)(g)(i)(II); 5 U.S.C. app. §8H(h)(1)(B).

[15] 50 U.S.C. §3517(d)(5)(g)(i)(III); 5 U.S.C. app. §8H(h)(1)(C).

[16] *See* 50 U.S.C. §3517(d)(5)(A); *see also* 5 U.S.C. app. §8H(a)(1)(A), (B).

[17] 50 U.S.C. §3517(d)(5)(A); 5 U.S.C. app. §8H(a)(1)(A), (B). Inspectors General are generally intended to provide independent, objective audits and investigations of agency operations, among other things. *See* 50 U.S.C. §3517(a); *see also* 5 U.S.C. app. §2. The Inspector General of the IC is responsible for, among other things, conducting independent investigations, inspections, and audits of programs and activities that the Director of National Intelligence is responsible for administering. 50 U.S.C. §3033(b).

[18] 50 U.S.C. §3517(d)(5)(B); 5 U.S.C. app. §8H(b).

[19] 50 U.S.C. §3517(d)(5)(B); 5 U.S.C. app. §8H(b).

[20] 50 U.S.C. §3517(d)(5)(C); 5 U.S.C. app. §8H(c). "Congressional intelligence committees" refers to the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence. 50 U.S.C. §3517(a)(4); 5 U.S.C. app. §8H(h)(2).

[21] 50 U.S.C. §3517(d)(5)(D)(i); 5 U.S.C. app. §8H(d)(1). When an employee contacts a committee member or employee directly, the committee member or employee "receives [the] complaint or information … in that member or employee's official capacity as a member or employee of that committee." 50 U.S.C. §3517(d)(5)(D)(iii); 5 U.S.C. app. §8H(d)(3).

[22] 50 U.S.C. §3517(d)(5)(D)(ii)(I); 5 U.S.C. app. §8H(d)(2)(A).

[23] 50 U.S.C. §3517(d)(5)(D)(ii)(II); 5 U.S.C. app. §8H(d)(2)(B).

to federal employees.[24] However, the ICWPA appears to afford IC whistleblowers fewer protections than the WPA affords non-intelligence whistleblowers. The WPA provides an employee with an individual right of action for prohibited retaliation, through which he can bring a claim against this agency in the Merit Systems Protection Board (MSPB).[25] The MSPB can then provide several remedies, including, but not limited to, returning the individual to the position he would have been in if retaliation had not occurred, awarding back pay, and awarding any reasonable and foreseeable consequential damages.[26] If an employee's claim is unsuccessful before the MSPB, the employee can appeal the MSPB's decision to the U.S. Court of Appeals for the Federal Circuit.[27]

Conversely, the ICWPA provides no explicit mechanism for remedying for retaliation stemming from disclosure of an urgent concern to Congress; it merely prescribes the process through which such disclosures can be made and allows employees and contractors to then use those disclosure procedures to inform Congress of any resulting improper retaliation. Further, the ICWPA expressly states that Inspector General and agency head action taken pursuant to the ICWPA is not subject to judicial review, unlike retaliation claims under the WPA.[28] In comparing the ICWPA's protections against the WPA's, some commentators have questioned the ICWPA's effectiveness at protecting intelligence whistleblowers from improper retaliation.[29]

# Presidential Policy Directive 19

President Obama issued PPD-19 on October 10, 2012, to ensure that IC employees can effectively report instances of waste, fraud, and abuse.[30] PPD-19 protects *employees* who engage in "protected disclosures" from certain types of adverse action by their employers. Thus, unlike the ICWPA, PPD-19's protections do not appear to extend to IC contractors. Under PPD-19, five types of disclosures fall under the umbrella of "protected disclosures." First, protected disclosures include employee disclosures to the agency Inspector General, Director of National Intelligence, IGIC, or supervisors within the employee's direct chain-of-command.[31] The employee must reasonably believe that disclosures to such persons evidence (1) a perceived violation of law, rule, or regulation; (2) gross mismanagement; (3) gross waste of funds; (4) abuse of authority; or (5) a

[24] The WPA, by its text, does not apply to employees of "the Federal Bureau of Investigation, the Central Intelligence Agency, the Defense Intelligence Agency, the National Geospatial-Intelligence Agency, the National Security Agency, the Office of the Director of National Intelligence, and the National Reconnaissance Office." 5 U.S.C. §2302(a)(2)(C).

[25] 5 U.S.C. §1221.

[26] *Id.* at (g)(1)(A). The MSPB is an independent, quasi-judicial government agency that, among other things, "adjudicat[es] Federal employee appeals of agency personnel actions …" 5 C.F.R. §1200.1.

[27] *See* 5 U.S.C. §1214(c).

[28] 50 U.S.C. §3517(d)(5)(F); 5 U.S.C. app. §8H(f).

[29] *See, e.g.,* Mary-Rose Papandrea, *Leaker Traitor Whistleblower Spy: National Security Leaks and the First Amendment*, 94 B.U. L. Rev. 449, 493 (2014) (observing that "… the ICWPA arguably fails to provide any real protection …"); *See* Richard Moberly, *Whistleblowers and the Obama Presidency: the National Security Dilemma*, 16 Emp. Rts. & Emp. Pol'y J. 51, 109 (2012) (detailing perceived gaps in the protections that the ICWPA affords intelligence whistleblowers).

[30] PPD-19 at 1. Presidential policy directives are binding on executive agencies and, in practice, can be equivalent to executive orders. *See Ctr. for Effective Gov't v. Department of State*, No. 13-0414, 2013 WL 6641262, at *2, n. 3 (D.D.C. Dec. 17, 2013) ("even though issued as a directive, the PPD-6 carries the force of law as policy guidance to be implemented by recipient agencies, and it is the functional equivalent of an Executive Order.").

[31] PPD-19 at 7.

specific and substantial threat to public health or safety.[32] Second, PPD-19 protects disclosures to congressional committees made pursuant to the ICWPA, discussed above.[33] Third, "protected disclosures" comprise any disclosure of a violation of PPD-19.[34] Fourth, protected disclosures include those made pursuant to an investigation or proceeding involving a violation of PPD-19.[35] Finally, the definition of "protected disclosures" generally includes disclosures to Inspectors General.[36]

Under PPD-19, intelligence agency[37] employees who make protected disclosures cannot consequently be subject to adverse personnel actions[38] or have their access to classified information negatively affected by an officer or employee of the agency.[39] PPD-19 required intelligence agencies to certify, within 270 days of its issuance, that they had internal procedures for reviewing allegations of wrongful personnel actions or impacts on access to classified information.[40] These procedures must provide for the protection of classified information and intelligence sources and methods.[41] PPD-19 requires that agency procedures permit agency Inspectors General to review employee allegations of adverse personnel action or improper restriction of access to classified information and recommend agency heads take corrective action if a violation of PPD-19 has occurred.[42] Such corrective action can include (but is not limited to) reinstatement, back pay, and attorney's fees.[43] Once an agency head receives an Inspector General's recommendation, PPD-19 requires he "carefully consider" the recommendation and findings and decide whether or not corrective action is appropriate.[44]

After employees exhaust the internal agency review process, PPD-19 allows them to request external review to the IGIC acting on behalf of the Director of National Intelligence.[45] Once such a request is made, the IGIC can, within his or her discretion, convene an external review panel.[46] Such a panel consists of the ICIG plus two Inspectors General that the ICIG chooses from the

[32] *Id*.

[33] *See id.*

[34] *Id.*

[35] *Id.* at 8.

[36] *Id.*

[37] More specifically, PPD-19 applies to so-called "Covered Agenc[ies]", which it defines as an executive department or independent establishment that contains an "Intelligence Community Element," including the Central Intelligence Agency, National Security Agency, Defense Intelligence Agency, National Geospatial-Intelligence Agency, National Reconnaissance Office, and any other agency that the President determines has as its principal function the conduct of foreign intelligence or counterintelligence activities. *Id.* at 6. The directive explicitly states that the Federal Bureau of Investigations *is not* a "Covered Agency." *Id*.

[38] Prohibited personnel actions include, but are not limited to, transfer, reassignment, demotion, suspension, termination, and negative decisions regarding pay or benefits. *Id.*

[39] *Id.* at 2-3.

[40] *Id.* PPD-19 mandates that such review processes apply to any actions arising after the date on which the intelligence agency head certifies the agency review process. *Id*.

[41] *Id.*

[42] *Id.*

[43] *Id.*

[44] *Id.*

[45] *Id.* at 4. The Director of National Intelligence is a presidential appointee "subject to the authority, direction, and control of the President" who, among other things, advises the President, National Security Council, and Homeland Security Council on intelligence matters related to national security. 50 U.S.C. §3023.

[46] PPD-19 at 4.

Departments of State, the Treasury, Defense, Justice, Energy, Homeland Security, or the CIA, exclusive of the Inspector General of the agency that internally reviewed the retaliation claim.[47] The panel then has 180 days to determine whether improper retaliation occurred.[48] If the panel concludes that such retaliation did happen, it can recommend that the agency head take corrective action, and the agency head must "carefully consider" this recommendation.[49] The agency head then has 90 days to inform the panel and the Director of National Intelligence of what, if any, action it takes.[50] The Director of National Intelligence must notify the President if the agency head does not tell the Director what action he takes within the allotted 90-day window.[51] PPD-19 further requires the IGIC to report annually all panel determinations and recommendations, along with agency head responses, to the Director of National Intelligence and, "as appropriate, to the relevant congressional committees."[52]

PPD-19 offers intelligence whistleblowers falling within its scope more protection against retaliation than the ICWPA. By allowing IC employees and contractors to disclose retaliation via adverse personnel action to congressional intelligence committees, the ICWPA purports to protect against only adverse personnel action; unlike PPD-19, it makes no mention of adverse security clearance determinations. Further, PPD-19, unlike the ICWPA, expressly prohibits retaliation against IC whistleblowers who make protected disclosures, whereas the ICWPA merely outlines the process through which such disclosures can be made.

Although PPD-19 offers intelligence whistleblowers more protection against retaliation than the ICWPA, it is unclear how effective PPD-19 will be in curbing such retaliation. Under PPD-19, the initial review of an improper retaliation allegation occurs within the agency wherein the whistleblower allegedly faced retaliation. This could raise questions regarding the initial review's impartiality, and thus effectiveness at achieving accurate results. Further, though PPD-19 appears to attempt to counteract impartiality in reviewing retaliation claims by creating an external review panel to whom such claims can eventually go, this external review panel cannot mandate that agency heads take corrective action after finding that impermissible retaliation occurred. Rather, this external review panel can only recommend that agency heads take corrective action. The agency head is then free to disregard the board's recommendation. Finally, as with all presidential policy directives or executive orders, President Obama (or any future Presidents) can revoke or modify it at any time.[53]

[47] *Id.*

[48] *Id.*

[49] *Id.*

[50] *Id.*

[51] *Id.*

[52] *Id.*

[53] See CRS Report RS20846, *Executive Orders: Issuance, Modification, and Revocation*, by (name redacted) and (name redacted).

# Title VI of the Intelligence Authorization Act for FY2014

On July 7, 2014, Congress enacted the Intelligence Authorization Act for FY2014,[54] which included protections for IC whistleblowers at Title VI of the act. Title VI seemingly codifies some of PPD-19's protections and, under specified circumstances, expands upon them. Like PPD-19, Title VI's protections extend only to *employees* of "covered intelligence community element[s],"[55] and therefore do not appear to apply to IC contractors.[56] Title VI's protections are bifurcated: it protects whistleblowers from retaliation in the form of both adverse personnel actions and adverse security clearance or information access determinations resulting from their making protected disclosures. Whether or not a disclosure is protected under Title VI depends on what is being disclosed to whom, and protected disclosures and enforcement mechanisms under the act differ in the context of retaliation via adverse personnel actions and adverse security clearance or information access determinations.

## Protection from Adverse Personnel Actions

Under Title VI, disclosures for which an employee is protected against retaliation in the form of adverse personnel action include those made to (1) the Director of National Intelligence (or his or her designee); (2) the IGIC (or his or her designee); (3) the head of the employing agency (or his or her designee); (4) the employing agency's Inspector General; (5) congressional intelligence committees; or (6) a member of a congressional intelligence committee.[57] For Title VI to protect an employee against adverse personnel action, the disclosure must be of information that the employee reasonably believes evidences a violation of federal laws or regulations, mismanagement, waste of funds, abuse of authority, or a substantial and specific danger to public health or safety.[58] Title VI does not contain any mechanism to enforce its protection against retaliation by adverse personnel action; it merely prohibits agency employees from taking adverse personnel action against other employees who make protected disclosures.[59] Enforcement is expressly left to the President.[60] It is unclear whether the President will develop new enforcement procedures, or will utilize enforcement procedures that already exist (i.e., PPD-19's enforcement procedures).

[54] P.L. 113-126, 128 Stat. 1390 (2014).

[55] Covered agencies include the Central Intelligence Agency, National Geospatial-Intelligence Agency, Office of the Director of National Intelligence, Defense Intelligence Agency, National Security Agency, and the National Reconnaissance Office. 50 U.S.C. §3234(a)(2).

[56] *See* 50 U.S.C. §3234(b); 50 U.S.C. §3341(j)(1).

[57] 50 U.S.C. §3234(b).

[58] *Id*.

[59] 50 U.S.C. §3234(b).

[60] 50 U.S.C. §3234(c).

## Protection from Adverse Security Clearance and Information Access Determinations

Under Title VI, an IC employee cannot take adverse security clearance action against another employee, or restrict the other employee's access to classified information, because the employee made a protected disclosure.[61] The disclosures for which an employee cannot face adverse security clearance actions or access determinations differ from the disclosures for which an employee cannot face adverse personnel actions.[62] In the context of adverse security clearance actions or access determinations, Title VI's umbrella of protected disclosures includes a number of lawful communications. First, it includes communications to the Director of National Intelligence, agency head, or agency Inspector General (or their respective designees) that the employee reasonably believes evidences a violation of federal laws or regulations, gross mismanagement, waste of funds, abuse of authority, or a substantial and specific danger to public health or safety.[63] Second, it includes disclosures made in accordance with the procedures outlined in the ICWPA, discussed above.[64] Finally, Title VI protects disclosures made while exercising a legal right of appeal or complaint (including testimony in connection with someone else exercising such a right) or cooperating with an Inspector General.[65] However, disclosures within this third category fall within Title VI only if they do not result in the sharing of information that is classified under an executive order for national security reasons.[66]

Title VI's protections against adverse security or information access determinations also differ from its protections against adverse personnel actions because it provides mechanisms for enforcing the former; whereas enforcement of the latter is left to the President's discretion as mentioned above. Title VI directed the President to select, within 180 days of the statute's enactment (July 7, 2014), an agency or department responsible for ensuring that intelligence agencies have adequate procedural protections that they must follow before taking action that adversely affects an employee's security clearance or information access.[67] Within this time frame, the President must also select an agency or department responsible for developing procedures that agencies must follow for employee appeals of adverse security clearance or information access decisions to the ICIG or agency Inspector General.[68] Title VI permits an employee 90 days from the adverse security clearance or information determination to use these appeal procedures.[69]

The appeal procedures that must be established under Title VI must allow the ICIG or agency Inspector General to engage in a fact-finding investigation and report the investigation results to the agency head within 180 days of the employee's appeal.[70] During the investigation, the

[61] 50 U.S.C. §3341(j)(1).

[62] *Compare* 50 U.S.C. §3234(b) *with* 50 U.S.C. §3341(j)(1)(A)-(D).

[63] 50 U.S.C. §3341(j)(1)(A),(B).

[64] 50 U.S.C. §3341(j)(1)(C).

[65] 50 U.S.C. §3341(j)(1)(D).

[66] *Id*.

[67] 50 U.S.C. §3341(b)(7)(B).

[68] 50 U.S.C. §3341(b)(7)(A); P.L. 113-126, §602(a)(2), 128 Stat. 1390, 1416-17 (2014).

[69] 50 U.S.C. §3341(j)(4)(A).

[70] P.L. 113-126, §602(a)(2), 128 Stat. 1390, 1416-17 (2014).

employee must be allowed, "to the fullest extent possible," to present relevant evidence.[71] The ICIG or agency Inspector General cannot find that a prohibited security clearance or information access determination occurred if the agency demonstrates that the employee's disclosure was not a contributing factor in the determination.[72] The agency can demonstrate such by establishing, by a preponderance of the evidence, that it would have taken the same action absent the employee's protected disclosures.[73] Under the preponderance of the evidence standard, it appears as though the agency must show that it is more likely than unlikely that the agency would have taken the same action against the employee absent the employee's disclosures.[74] In evaluating the agency's contributing factor evidence, Title VI requires the ICIG or agency Inspector General to afford the "utmost deference" to the agency's judgments regarding threats to national security.[75] If the ICIG or agency Inspector General determines that a prohibited security clearance or information access determination occurred and reports its determination to the agency head, the agency head "shall" take corrective action.[76]

If, however, the ICIG or agency Inspector General finds that no improper adverse security clearance or information access determination occurred, Title VI requires that the employee be given 60 days to externally appeal such a finding.[77] Title VI does not contain substantive requirements for this external appeal.[78] Rather, through the statute, Congress mandated that the Director of National Intelligence, in consultation with the Attorney General and the Secretary of Defense, develop and implement procedures for adjudicating external appeals.[79] As of this writing, the Director of National Intelligence does not appear to have developed these appeal procedures. Though Title VI does not contain substantive requirements for appeal procedures, it does require the Director of National Intelligence to inform the congressional intelligence committees when he issues an appeal order under the procedures that he develops.[80]

Title VI seemingly expands PPD-19's protections against retaliation in the form of adverse security clearance or information access determinations by introducing additional enforcement mechanisms. For example, Title VI requires adequate protections prior to adverse security clearance or information access determinations, where PPD-19 does not. However, Title VI does not appear to strengthen PPD-19's protections against retaliation in the form of adverse personnel action, as it leaves enforcement of such protections to the President.

---

[71] *Id*.

[72] 50 U.S.C. §3341(j)(4)(C).

[73] *Id*.

[74] *See Concrete Pipe and Prods. of Cal v. Constr. Laborers Pension Trust of S. Cal.*, 508 U.S. 602, 622 (observing that showing a fact by a preponderance of the evidence "simply requires the trier of fact to believe that the existence of a fact is more probable than its nonexistence …") (internal quotations omitted).

[75] *Id*.

[76] 50 U.S.C. §3341(j)(4)(B). This corrective action must, as "nearly as practicable and reasonable," put the employee in the position he would have been in but-for the prohibited retaliation and can include compensatory damages of up to $300,000. *Id*.

[77] 50 U.S.C. §3341(j)(5)(A).

[78] *See id*.

[79] 50 U.S.C. §3341(j)(5)(B).

[80] 50 U.S.C. §3341(j)(5)(C).

## Author Contact Information

(name redacted)
Legislative Attorney
[redacted]@crs.loc.gov, 7-....