



**Congressional
Research Service**

Informing the legislative debate since 1914

Intelligence Community Whistleblower Provisions: A Legislative History

Updated March 29, 2024

Congressional Research Service

<https://crsreports.congress.gov>

R45345



R45345

March 29, 2024

Michael E. DeVine
Analyst in Intelligence and
National Security

Intelligence Community Whistleblower Provisions: A Legislative History

Intelligence community (IC) whistleblowers are employees or contractors of the federal government working in any of the 18 elements of the IC who disclose their reasonable belief of a violation of law, rule, or regulation; gross mismanagement; waste of resources; abuse of authority; or a substantial danger to public health and safety. The Director of National Intelligence (DNI) whistleblowing policy and guidance generally are publicly available, and address the process for making protected disclosures and identify whistleblower protections for IC contractors, members of the Armed Forces, and federal IC employees.

IC whistleblower protections have evolved in response to perceptions of gaps that some observers argued left these whistleblowers vulnerable to reprisal. The first whistleblower legislation specific to the IC, enacted in 1998, was limited to specifying a process for IC whistleblowers to make a complaint but offered no specific protections. Subsequent legislation, enacted in 2010, included general provisions for protecting IC whistleblowers, with no additional guidance on standards for implementation. Presidential Policy Directive (PPD)-19, signed in 2012, provided the first specific protections against reprisal actions for making a complaint. The Intelligence Authorization Act for Fiscal Year 2014 (P.L. 113-126) codified these provisions, which were further supported by IC implementation policy. In early 2018, Congress passed legislation to address perceived gaps in protections for IC contractors. Other provisions in Title 10 of the U.S. Code, along with Department of Defense (DOD) implementing guidance, provide protections for members of the Armed Forces, including those assigned to elements of the IC.

The August 2019 whistleblower complaint by a member of the IC that led to the impeachment of President Donald J. Trump raised additional questions among many in Congress about whether existing statutory protections are sufficient. These questions concerned (1) whether whistleblowers should have a right to remain anonymous, and, if so, what, if any, recourse should they have in the event their identities are disclosed against their will; (2) whether procedures provide potential whistleblowers clear direction on how to approach Congress with a protected disclosure; (3) whether the text of the various IC-related whistleblower statutes is clear and consistent as they relate to each other; and (4) which official has the final authority for making a determination of, as well as the scope of, an activity that constitutes a matter of “urgent concern.”

Since that time, Congress has taken steps to provide greater clarity and consistency to existing whistleblower legislation which address each of these questions. The Intelligence Authorization Act (IAA) for Fiscal Year 2022 (Division X of P.L. 117-103), included, for example, a provision giving the Inspector General of the Intelligence Community (ICIG) and Inspectors General of any IC element sole authority to determine whether a protected disclosure constitutes a matter of “urgent concern.”

Effective whistleblowing protections are intended to instill confidence in the integrity and comprehensiveness of the process for submitting a complaint as much as for the process itself. By extension, when IC employees have confidence that they can make protected disclosures anonymously and without fear of retribution, they arguably are more likely to adhere to a process that is also intended to protect classified information. Conversely, this line of reasoning also suggests that a lack of confidence can increase the chances of wrongdoing going unreported or of classified information being compromised through an employee making a complaint outside of proper channels.

Contents

Introduction	1
Evolution of Whistleblower Protection Laws and Policy.....	3
Intelligence Community Whistleblower Protection Act (ICWPA) of 1998	3
Intelligence Authorization Act (IAA) for Fiscal Year 2010	6
Presidential Policy Directive (PPD)-19.....	8
Title VI of the Intelligence Authorization Act (IAA) for Fiscal Year 2014	9
Intelligence Community Directive (ICD)-120	10
Whistleblower Protections for Members of the Armed Forces Assigned to the IC	11
Legislation to Address Perceived Gaps in Protections for IC Contractors.....	12
Issues Raised by the IC Whistleblower Complaint of August 2019.....	13
117 th Congress: Intelligence Authorization Act for Fiscal Year 2022	15
Selected Provisions	15
Issues for Congress	16

Contacts

Author Information.....	17
-------------------------	----

Introduction

Intelligence community (IC) whistleblowers are employees or contractors working in any of the statutory elements of the IC who disclose a reasonable belief of a violation of law, rule, or regulation; gross mismanagement; waste of resources; abuse of authority; or a substantial danger to public health and safety. One important distinction between whistleblowers generally and those in the IC (or those who otherwise have security clearances) is the concern for protecting classified information that may be involved in an IC-related incident or complaint. The IC has recognized that whistleblowing can help ensure an ethical and safe working environment, and enable timely responses for corrective action.¹

Congress and the executive branch have defined, in statute and directives, procedures for IC whistleblowers to make protected disclosures that also provide for the security of classified information.² The Director of National Intelligence (DNI) whistleblowing policy and guidance are publicly available and specifically address whistleblower processes and protections for IC contractors, members of the Armed Forces, and federal employees.³ Some proponents for greater transparency in the IC, however, have said the IC's internal processes are not as clear as they could be and lack the transparency necessary to provide prospective whistleblowers confidence that they would be protected against reprisal.

Procedures for an intelligence community employee to make a protected disclosure are codified in three statutes:

- the Inspector General Act of 1978, as amended (5 U.S.C. §416), which specifies procedures for making a protected disclosure to various inspectors general of intelligence community elements;⁴
- the Central Intelligence Agency (CIA) Act of 1949, as amended (50 U.S.C. §3517), which provides procedures for employees of the CIA to make a protected disclosure to the Inspector General of the CIA; and
- the National Security Act of 1947, as amended (50 U.S.C. §3033), which provides procedures for whistleblowers in the Office of the Director of National Intelligence (ODNI) or any element of the intelligence community to make a protected disclosure to the Intelligence Community Inspector General (ICIG).

IC whistleblower *protections* have evolved in response to perceptions of gaps that some believed left whistleblowers vulnerable to reprisal. Protections for an employee making a protected disclosure are found in Title VI of the Intelligence Authorization Act for Fiscal Year 2014, as amended (50 U.S.C. §§3234 et seq.). This statute codified the provisions of Presidential Policy Directive (PPD)-19 signed by President Barack Obama in 2012.

Whistleblower protections for employees and contractors in the IC are extended only to those who makes protected disclosures. They do not cover disclosures that do not conform to statutes and directives prescribing reporting procedures intended to protect classified information, for

¹ Office of the Director of National Intelligence (ODNI), at <https://www.dni.gov/ICIG-Whistleblower/index.html>.

² Intelligence community whistleblower statutes and directives use the terms “protected disclosure” and “lawful disclosure” interchangeably. This report uses the term “protected disclosure” for consistency.

³ Office of the Director of National Intelligence, *How Do I Report?* at <https://www.dni.gov/ICIG-Whistleblower/process-how.html>.

⁴ Following reordering and renumbering of the Inspector General Act of 1978 in the U.S. Code, 5 U.S.C. App. §8H, “Additional Provisions with Respect to Inspectors General of the Intelligence Community,” is now codified at 5 U.S.C. §416.

example, by disclosing classified information to the media or a foreign government. The whistleblower protections do not apply to personal grievances, policy disputes, or management disagreements.⁵ Whistleblower protections also do not protect against adverse personnel or security clearance eligibility decisions if the agency can demonstrate “by a preponderance of the evidence” that it would have taken the same action in the absence of a protected disclosure.⁶

The August 2019 whistleblower complaint that led to the impeachment of President Donald J. Trump revealed a number of different ways that IC whistleblowing statutes could be interpreted. Some in Congress questioned the independence of IC inspectors general to make a final determination of whether a complaint is credible and a matter of “urgent concern.”⁷ In addition, there was informal discussion over whether the statute should provide comprehensive protections against disclosure of a whistleblower’s identity.⁸ The Intelligence Authorization Act for Fiscal

⁵ Office of the Director of National Intelligence, *What is Whistleblowing?* at <https://www.dni.gov/ICIG-Whistleblower/what-is.html>.

⁶ 50 U.S.C. §3341(j)(4)(C).

⁷ A provision in the Intelligence Authorization Act (IAA) for Fiscal Year 2022 resolved the uncertainty over the independence and authority of the Inspector General of the Intelligence Community (ICIG) and inspectors general of IC elements. The IAA for FY2022 amended 50 U.S.C. §§3033(k)(5)(G) and 3517(d)(5)(G) and 5 U.S.C. §416 to provide the inspectors general “sole authority” to decide whether a complaint is a matter of urgent concern.

⁸ The Inspector General Act of 1978 (5 U.S.C. §407(b)) prohibits an inspector general from disclosing the identity of an employee making a complaint, such as a whistleblower, to the extent practicable:

The Inspector General shall not, after receipt of a complaint or information from an employee, disclose the identity of the employee without the consent of the employee, unless the Inspector General determines such disclosure is unavoidable during the course of the investigation.

The whistleblowing provision pertaining to the ICIG, 50 U.S.C. §3033(k)(5)(H), makes no specific reference to protecting a whistleblower’s identity from disclosure, but states that “nothing in this section shall be construed to limit the protections afforded to an employee under ... section 8H of the Inspector General Act of 1978 (5 U.S.C. App.)” However, 50 U.S.C. §3033 (pertaining to the ICIG), 50 U.S.C. §3517 (pertaining to the Inspector General of the CIA), and 5 U.S.C. §416 (pertaining to inspectors general of IC elements generally, formerly numbered as 5 U.S.C. App. §8H), are not applicable to anyone other than the inspector general of the IC element handling a complaint. They do not afford protection to whistleblowers against disclosure of their identity by someone other than the inspector general, such as a member of the media or a Member of Congress if such an individual who is not an inspector general were to become aware of the whistleblower’s identity.

There are two exceptions to the prohibitions against the ICIG disclosing a whistleblower’s identity: (1) in instances where an IG determination that disclosure is “unavoidable” in the course of the investigation; or (2) when disclosure to a Department of Justice official is “responsible for determining whether a prosecution should be undertaken” (50 U.S.C. §3033(g)(3)(A)). However, 50 U.S.C. §3033(g)(3)(A) also states that the provision “*shall qualify as a withholding statute pursuant to subsection (b)(3) of section 552 of Title 5,*” of the Freedom of Information Act (FOIA). FOIA’s mandatory disclosure requirements under 5 U.S.C. §552(b)(3) state that they do not apply to covered materials “specifically exempted from disclosure by statute” in specified circumstances. Section 3033, therefore, obligates an IC inspector general to protect a whistleblower’s identity from disclosure under FOIA. For more information on FOIA, CRS In Focus IF12301, *Congress and the Freedom of Information Act (FOIA)*, by Benjamin M. Barczewski and Meghan M. Stuessy. See also CRS Report R46238, *The Freedom of Information Act (FOIA): A Legal Overview*, by Daniel J. Sheffner.

Information associated with whistleblowers’ communications is or may be contained in a system of records governed by the Privacy Act. See ODNI/OIG-003, 76 *Federal Register* 42749, July 19, 2011, at <https://www.govinfo.gov/content/pkg/FR-2011-07-19/pdf/2011-18193.pdf>. The Privacy Act states, “No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains.” 5 U.S.C. §552a(b). The act contains several exceptions to this mandate, including one governing disclosure to Congress. 5 U.S.C. §552a(b)(9).

One additional variable involves statutory protections against disclosing the identity of a case officer or other officer of the IC working in a protected status (50 U.S.C. §3121, *Protection of Identities of Certain United States Undercover* (continued...))

Year 2022 (Division X of P.L. 117-103) has addressed some of the concerns raised by the 2019 whistleblowing incident, such as the provision that gave the inspectors general of IC elements “sole authority” for determining whether a protected disclosure constitutes a matter of “urgent concern.”

When Congress initially drafted the statutes related to intelligence community whistleblowing, beginning in 1998, there were some inconsistencies in language that since have been resolved through amending legislation. This report addresses several of these amendments, particularly as they relate to the definition of a matter of “urgent concern,” the independence of the IC inspectors general, and the language of the overall framework for whistleblower protections in PPD-19.⁹

For members of the Armed Forces assigned to elements of the IC, 10 U.S.C. §1034 provides whistleblower protections. Department of Defense (DOD) implementing guidance for Section 1034 can be found in DOD Directive 7050.06, *Military Whistleblower Protection*.¹⁰

Evolution of Whistleblower Protection Laws and Policy

Intelligence Community Whistleblower Protection Act (ICWPA) of 1998

The Intelligence Community Whistleblower Protection Act of 1998 (ICWPA),¹¹ as amended, is intended to assist whistleblowers in the IC, all of whom are specifically excluded from the Whistleblower Protection Act of 1989, which applies solely to federal employees outside of the IC who work in an unclassified environment.¹² The ICWPA amended the CIA Act of 1949 and the Inspector General Act of 1978 to enable any IC federal employee or contractor “who intends to report to Congress a complaint or information with respect to an urgent concern” to report to the Inspector General (IG) of the employee’s or contractor’s IC agency. The ICWPA, as amended, defines an “urgent concern” as

(A) a serious or flagrant problem, abuse, violation of law or executive order, or deficiency relating to the funding, administration, or operations of an intelligence activity of the Federal Government that is a matter of national security, and not a difference of opinion concerning public policy matters;¹³

Intelligence Officers, Agents, Informants, and Sources). This provision also includes an exception for disclosure to Congress.

⁹ For a more detailed look at the effort to synchronize the language of IC whistleblower legislation, see Office of the Inspector General of the Intelligence Community, “Report on Intelligence Community Whistleblower Matters & Harmonization of Processes and Procedures,” March 4, 2021, at <https://www.dni.gov/files/ICIG/Documents/Publications/Reports/2021/IC%20IG%205333-6713%20Report.pdf>.

¹⁰ DODD 7050.06, incorporating Change 1, October 12, 2021, at <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/705006p.pdf>.

¹¹ Title VII of the IAA for Fiscal Year 1999, P.L. 105-272, §§701-702, codified in 5 U.S.C. §416, 50 U.S.C. §3033, and 50 U.S.C. §3517.

¹² The ICWPA makes no provision for members of the Armed Forces assigned to an IC element; 10 U.S.C. §1034 provides whistleblower protections for members of the Armed Forces, including those who may be assigned to an element of the IC.

¹³ The definition for a matter of “urgent concern” as it pertains to the IC is found in three statutes: 50 U.S.C. §3517(d)(5)(G)(i)(aa), pertaining to the Inspector General of the CIA; 5 U.S.C. §416(a)(2), pertaining to the Inspectors (continued...)

(B) a false statement to the Congress, or a willful withholding from Congress on an issue of material fact relating to the funding, administration, or operation of an intelligence activity;¹⁴ or

(C) an action ... constituting reprisal or threat of reprisal ... in response to an employee's reporting of an urgent concern.¹⁵

In 1998, Congress noted that the prior absence of a statutory IC whistleblower protection mechanism “may have impaired the flow of information needed by the intelligence committees to carry out oversight responsibilities.”¹⁶ Consequently, the ICWPA defines the formal processes for submitting complaints to ensure the protection of any classified information:¹⁷

- A designee of the IG who receives a complaint of an urgent concern from an employee has seven days from receipt to report the complaint to the intelligence element's IG.¹⁸
- Not later than 14 calendar days from receipt, the responsible IG must report all complaints that the IG determines are credible to the head of the intelligence element, along with all supporting material.¹⁹
- Within seven days of receipt, the head of the intelligence element is required to report the complaint to the congressional intelligence committees along with any comments the intelligence element considers appropriate.²⁰
- If the head of the intelligence element determines that the complaint would create a conflict of interest for him/her, that individual will return the complaint to the intelligence element's IG who will forward it to the Director of National Intelligence, or, for the four DOD intelligence agencies, to the Secretary of Defense for forwarding to the congressional intelligence committees.²¹

General of intelligence community elements generally; and 50 U.S.C. §3033(k)(5)(G)(i), pertaining to the Inspector General of the Intelligence Community (ICIG). As currently written, the definition is substantively equal across the statutes. The Intelligence Authorization Act (IAA) for Fiscal Year 2023 (Division F of P.L. 117-263) amended the definition of “urgent concern” in all three statutes by no longer specifying that a matter of urgent concern had to involve classified information. In addition, the IAA for FY23 amended the statute concerning the ICIG by specifying that a matter of urgent concern handled by the ICIG no longer had to be “within the responsibility and authority of the Director of National Intelligence.” This amendment broadened the scope of what could be reported to the ICIG by enabling a whistleblower to make a protected disclosure about a matter of urgent concern related to an activity of importance to U.S. national security generally, rather than simply concerning a matter under the authority of the DNI.

¹⁴ 5 U.S.C. §416(a)(2)(B), 50 U.S.C. §3033(k)(5)(G)(ii), 50 U.S.C. §3517(d)(5)(G)(i)(bb).

¹⁵ 5 U.S.C. §416(a)(2)(C), 50 U.S.C. §3033(k)(5)(G)(iii), 50 U.S.C. §3517(d)(5)(G)(i)(I)(cc).

¹⁶ P.L. 105-272, §702.

¹⁷ The process for submitting a whistleblower complaint in the IC is codified at 5 U.S.C. §416(c)(1), 50 U.S.C. §3033(k)(5)(B), and 50 U.S.C. §3517(d)(5).

¹⁸ The IGs of the IC agencies within the DOD—the Defense Intelligence Agency, National Geospatial-Intelligence Agency, National Reconnaissance Office, and National Security Agency—are designees of the DOD IG. See 5 U.S.C. §416(b)(2) and (3). An individual submitting a complaint to an Inspector General of any of these agencies may notify a Member of either of the congressional intelligence committees of the fact that a complaint has been submitted and the date of submission to the IG. See 5 U.S.C. §416(h). “Element” is the term used in statute to designate each of the 18 specific agencies or organizations within the intelligence community.

¹⁹ 5 U.S.C. §416(c)(1), 50 U.S.C. §3033(k)(5)(B), 50 U.S.C. §3517(d)(5)(B)(i).

²⁰ 5 U.S.C. §416(d), 50 U.S.C. §3033(k)(2)(B), 50 U.S.C. §3517(d)(5)(C).

²¹ 5 U.S.C. §416(c)(2), 50 U.S.C. §3517(d)(5)(B)(2). The four DOD intelligence agencies are the National Security Agency, the National Reconnaissance Office, the National Geospatial-Intelligence Agency, and the Defense Intelligence Agency.

- In the event the IG does not report the complaint, does not find it credible, or reports it inaccurately, the complainant has the right to submit the complaint to either or both of the congressional intelligence committees directly.²²
- If the complainant chooses to report directly to Congress, he/she must first provide a statement to the head of the intelligence element via the element's IG, providing notice of his/her intent to contact the congressional intelligence committees directly. Moreover, the complainant must follow the head of the intelligence element's guidance on security and the protection of classified material.²³
- The intelligence element's IG will notify the employee making the complaint of any action involving the complaint within three days of taking the action. None of the actions taken by the intelligence element in handling a complaint in accordance with provisions in statute are subject to judicial review.²⁴

Although the ICWPA provides a process for IC whistleblowers—employees and contractors—to report complaints to Congress securely via the IG of the whistleblower's IC agency, it offers no specific provisions for protecting whistleblowers from reprisal or punishment. Subsequent legislation that specifically prohibits actions taken in reprisal for an IC employee making a protected disclosure (a disclosure that adheres to the ICWPA process for making a complaint while protecting classified information) underscores the perception that the ICWPA process alone did not adequately protect a whistleblower against adverse personnel action.

The ICWPA provides an additional dimension of congressional oversight. The intent of the statute is to “encourage” an IC complainant to report to Congress via an established process that provides for the protection of classified information.²⁵ Informing Congress was not contingent only upon the appropriate authority deciding a complaint constituted a “matter of urgent concern.” The statute provides a process for a complainant to inform the congressional intelligence committees even in the event the relevant IC element determines the complaint does not constitute a matter of urgent concern.²⁶

The law's findings, for instance, state that “Congress ... has a ‘need to know’ of allegations of wrongdoing within the executive branch, including allegations of wrongdoing in the Intelligence Community.”²⁷ The findings acknowledge that employees and contractors may be reluctant to report potentially serious problems out of fear of reprisal, impeding the flow of information, and complicating Congress's oversight responsibilities.²⁸ In other words, Congress appears to have wanted to establish a means for a member of the IC to report allegations of wrongdoing, whether or not the allegations were determined to be matters of urgent concern, so long as the process allowed for the protection of classified information.

²² 5 U.S.C. §416(e)(1), 50 U.S.C. §3033(k)(5)(D)(i); 50 U.S.C. §3517(d)(5)(D)(i).

²³ 5 U.S.C. §416(e)(2), 50 U.S.C. §3033(k)(5)(D)(ii); 50 U.S.C. §3517(d)(5)(D)(ii).

²⁴ 5 U.S.C. §416(f)-(g); 50 U.S.C. §3033(k)(5)(E)-(F); 50 U.S.C. §3517(d)(5)(E)-(F).

²⁵ P.L. 105-272§701(b)(6).

²⁶ Section 701(b)(6) of H.Rept. 105-780, *Conference Report for the Intelligence Authorization Act for Fiscal Year 1999*.

²⁷ Section 701(b)(3) of the Conference Report to accompany P.L. 105-272 105th Cong., 2nd sess., H.Rept. 105-780, October 5, 1998.

²⁸ Section 701(b)(5) of the Conference Report to accompany P.L. 105-272 105th Cong., 2nd sess., H.Rept. 105-780, October 5, 1998.

Intelligence Authorization Act (IAA) for Fiscal Year 2010

The IAA for FY2010 (P.L. 111-259), included the first general provisions for protection of IC whistleblowers as part of legislation that established the Office of the Inspector General of the Intelligence Community (OIGIC), headed by the ICIG. Section 405(a)(1) of the IAA for FY2010 added a new Section 103H to the National Security Act of 1947, which was codified as 50 U.S.C. §3033. This provision permits protected disclosures to the ICIG and echoes the ICWPA's provision protecting the whistleblower's identity from disclosure, but otherwise lacks the specificity of later whistleblower protection legislation and directives:

The Inspector General [of the Intelligence Community] is authorized to receive and investigate ... 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. Once such complaint or information has been received from an employee of the intelligence community—

(A) the Inspector General shall not disclose the identity of the employee without the consent of the employee, unless the Inspector General determines that such disclosure is unavoidable during the course of the investigation or the disclosure is made to an official of the Department of Justice responsible for determining whether a prosecution should be undertaken, and this provision shall qualify as a withholding statute pursuant to subsection (b)(3) of section 552 of title 5 (commonly known as the "Freedom of Information Act");

(B) no action constituting a reprisal, or threat of reprisal, for making such complaint or disclosing such information to the Inspector General may be taken by any employee in a position to take such actions, unless the complaint was made or the information was disclosed with the knowledge that it was false or with willful disregard for its truth or falsity.²⁹

Section 405(K)(5)(A) of the IAA for FY2010 applies to any IC whistleblower, which includes contractors in addition to federal employees of IC elements.³⁰

Section 425(d) of the IAA for FY2010 amended the CIA Act of 1949 to clarify existing protections against reprisals involving CIA employees who make protected disclosures to the CIA Inspector General.³¹

Finally, the FY2010 IAA provides a means for addressing differences that may arise between the ICIG and the DNI. Specifically, Section 405 gives the DNI authority to prohibit the ICIG from "initiating, carrying out, or completing any investigation, inspection, audit, or review if the Director determines that such prohibition is necessary to protect vital national security interests of the United States."³² In such situations, the DNI must submit to the congressional intelligence committees within seven days of such determination a statement explaining the reasons.³³ The DNI must provide a copy to the ICIG, who may then submit comments on the statement to the

²⁹ 50 U.S.C. §3033(g)(3).

³⁰ Section 405(k)(5)(A) of P.L. 111-259, codified at 50 U.S.C. §3033(k)(5)(A). 50 U.S.C. §3033(g)(2)(B) also provides: "The Inspector General shall have access to any employee, or any employee of a contractor, of any element of the intelligence community needed for the performance of the duties of the Inspector General."

³¹ P.L. 111-259, §425(d). The provisions for prohibiting reprisal actions for protected whistleblower disclosures to the CIA Inspector General can be found in 50 U.S.C. §3517(e)(3)(A)-(B).

³² Codified at 50 U.S.C. §3033(f)(1).

³³ Codified at 50 U.S.C. §3033(f)(2).

congressional intelligence committees.³⁴ The ICIG shall “immediately notify, and submit a report to the congressional intelligence committees in the event that:”³⁵

- the DNI and ICIG cannot resolve a difference between them;³⁶
- an inspection, audit, or review focuses on any current or former senior IC official;³⁷
- the matter requires the ICIG to submit a report to the Department of Justice on possible criminal conduct by a senior intelligence official;³⁸
- the ICIG receives notice from the Department of Justice declining or approving prosecution of possible criminal conduct of any such official;³⁹ or
- the ICIG, “after exhausting all possible alternatives,” is unable to obtain significant documentary information in the course of an investigation, inspection, audit or review.⁴⁰

An IC employee or contractor who has submitted a complaint to the IG may notify any Member of either congressional intelligence committee, or a staff member of either committee, of the fact that the employee has made a complaint to the IG and the date of submission.⁴¹ In addition, the DNI must submit to the congressional intelligence committees any report on an investigation, audit, inspection, or review if requested by either the Chair or Vice Chair of the Senate intelligence committee, or the Chair or Ranking Member of the House intelligence committee.⁴²

³⁴ Another means by which Congress might potentially be prevented from being informed of a complaint involves claims of executive privilege. This report does not address this issue, although Presidents have claimed constitutional authority to review and limit, as necessary, the disclosure of classified or other sensitive information to Congress. See Robert S. Litt, “Unpacking the Intelligence Community Whistleblower Complaint,” *Lawfare*, September 17, 2019, at <https://www.lawfareblog.com/unpacking-intelligence-community-whistleblower-complaint>. See also Margaret Taylor, “The Mysterious Whistleblower Complaint: What is Adam Schiff Talking About,” *Lawfare*, September 17, 2019, at <https://www.lawfareblog.com/mysterious-whistleblower-complaint-what-adam-schiff-talking-about>.

³⁵ 50 U.S.C. §3033(k)(3)(A). For the 2019 IC whistleblower complaint against President Donald J. Trump, the ICIG provided notice to Congress as required by this provision in statute after the DNI informed the ICIG that he was unable to forward the complaint to Congress upon being informed by the White House Counsel’s Office that much of the complaint was protected from disclosure by executive privilege. See *Opening Statement by Acting Director of National Intelligence Joseph Maguire before the House Permanent Select Committee on Intelligence*, September 26, 2019, at <https://www.c-span.org/video/?464509-1/acting-director-national-intelligence-maguire-testifies-whistleblower-complaint>. The Office of the Director of National Intelligence (ODNI) also consulted the Department of Justice (DOJ) Office of Legal Counsel (OLC) on whether the complaint met the statutory definition of “urgent concern.” In its reply, the OLC gave its opinion that the President was not a member of the IC, that communications between the President and a foreign leader did not constitute an intelligence activity, and that, therefore, the complaint did not fall within the statutory definition of “urgent concern.” The opinion concluded that the acting DNI, therefore, was not legally required to forward the complaint to Congress. See Steven A. Engel, Assistant Attorney General Office of Legal Counsel, *Memorandum of Opinion for the General Counsel Office of the Director of National Intelligence*, September 3, 2019, at <https://www.justice.gov/olc/opinion/file/1205711/download>.

³⁶ 50 U.S.C. §3033(k)(3)(A)(i).

³⁷ 50 U.S.C. §3033(k)(3)(A)(ii) specifies the intelligence officials who would be subject to an audit, investigation, or inspection over which the DNI and ICIG might disagree, and which would require reporting to Congress, to include current or former intelligence officials appointed by the President or the DNI, or a head of any IC element, including those serving in an acting capacity.

³⁸ 50 U.S.C. §3033(k)(3)(A)(iii).

³⁹ 50 U.S.C. §3033(k)(3)(A)(iv).

⁴⁰ 50 U.S.C. §3033(k)(3)(A)(v).

⁴¹ 50 U.S.C. §3033(k)(5)(I). This is limited to notification of the fact, and date, of a complaint being made. It differs from a whistleblower submitting a complaint directly to Congress which is governed by 50 U.S.C. §3033(k)(5)(D)(ii).

⁴² 50 U.S.C. §3033(k)(4).

Presidential Policy Directive (PPD)-19

PPD-19, *Protecting Whistleblowers with Access to Classified Information*, signed by President Obama on October 10, 2012, provided the first executive branch regulatory framework of protections for IC whistleblowers. PPD-19 specifically protects some employees in the IC with access to classified information from personnel actions taken, or threatened to be taken, in reprisal for making a protected disclosure.⁴³

PPD-19 defines a protected disclosure, in part, as follows:

a disclosure of information by the employee to a supervisor in the employee's direct chain of command up to and including the head of the employing agency, to the Inspector General of the employing agency or Intelligence Community Element, to the Director of National Intelligence, to the Inspector General of the Intelligence Community, or to an employee designated by any of the above officials for the purpose of receiving such disclosures, that the employee reasonably believes evidences (i) a violation of any law, rule, or regulation; or (ii) gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety.⁴⁴

PPD-19 also

- Prohibits reprisals that (1) could affect a whistleblower's eligibility for access to classified information; or (2) involve a personnel action against the IC employee making a protected disclosure.⁴⁵
- Requires IC elements to certify to the DNI a process for IC employees to seek a review of personnel actions the employee believes constitute reprisal for making a protected disclosure. The review process also must provide for the security of classified information involved in a disclosure.

⁴³ Para. F(4) of PPD-19 defines a personnel action as,

an appointment, promotion, detail, transfer, reassignment, demotion, suspension, termination, reinstatement, restoration, reemployment, or performance evaluation; a decision concerning pay, benefits, or awards; a decision concerning education or training if the education or training may reasonably be expected to lead to an appointment, reassignment, promotion, or performance evaluation; a decision to order psychiatric testing or examination; and any other significant change in duties, responsibilities, or working conditions. (PPD-19, *Protecting Whistleblowers with Access to Classified Information*, The White House, October 10, 2012, at <https://www.opm.gov/our-inspector-general/whistleblower-protection-information/ppd-19.pdf>.)

PPD-19 otherwise does not define *employee* and does not include any reference to IC contractors. To some this was an important omission. In 2013, Edward Snowden, a Booz Allen Hamilton contractor working at the National Security Agency, went outside official channels to leak classified documents to the media claiming that official channels provided no protections for someone with his status as a contractor to submit a whistleblowing complaint. The ICWPA, which provides a *process* for submitting a whistleblowing complaint (but does not specify protections against prohibited reprisals), applies to contractors as well as federal IC employees. However, it was not until January 19, 2018, when Congress passed P.L. 115-118 (which included Section 110 covered later in this report), that contractors were also afforded specific protections from reprisals subsequent to submitting a complaint. For background on whistleblowing provisions related to Edward Snowden, see Joe Davidson, "No Whistleblower Protections for Intelligence Contractors," *Washington Post*, June 19, 2013, at https://www.washingtonpost.com/politics/federal_government/no-whistleblower-protections-for-intelligence-contractors/2013/06/19/dc3e1798-d8fa-11e2-a9f2-42ee3912ae0e_story.html.

⁴⁴ Presidential Policy Directive (PPD)-19, *Protecting Whistleblowers with Access to Classified Information*, The White House, October 10, 2012, https://www.dni.gov/ICIG-Whistleblower/resources/PPD_19.pdf.

⁴⁵ Adverse personnel actions might include demotion, transfer, termination, suspension, lower performance evaluation or punitive changes in duties and responsibilities.

- Requires, as part of the review process, that the IC element inspector general determine whether a personnel action was taken in reprisal for a protected disclosure. The IG may then make recommendations for corrective action in the event of a determination that a violation took place.
- Requires that the agency head “shall carefully consider the findings of and actions recommended by the agency Inspector General.” The agency head does not have to accept an IG’s recommendation for corrective action.
- Requires IC agencies to certify to the DNI that the agency has a review process that permits employees to appeal actions involving eligibility for access to classified information that are alleged to be in violation of prohibitions against retaliation for making protected disclosures.
- Allows for a whistleblower to request an external review by an IG panel chaired by the ICIG if the employee has exhausted the agency review process. In the event the panel decides in the employee’s favor, the agency must consider but does not have to accept the panel’s recommendation for corrective action.
- Requires the ICIG to report annually to the congressional intelligence committees the IG determinations and recommendations and IC element head responses to the determinations and recommendations.
- Requires the executive branch to provide training to employees with access to classified information (not including contractors or members of the Armed Forces) regarding protections for whistleblowers.
- Provides for a three-member External Review Panel, chaired by the ICIG, for an employee claiming reprisal and who has exhausted all other review processes. The ICIG has the discretion whether to convene an External Review Panel, which, if convened, shall complete a review of the claim within 180 days.⁴⁶

Title VI of the Intelligence Authorization Act (IAA) for Fiscal Year 2014

Title VI of the FY2014 IAA (P.L. 113-126), enacted on July 7, 2014, codified protections in PPD-19 (at 50 U.S.C. §3234) including the first expansive statutory protections for IC whistleblowers against personnel or security clearance actions made in reprisal for protected disclosures.⁴⁷

Section 601 of Title VI protects IC federal employee whistleblowers from any personnel action committed or omitted in retaliation for a protected disclosure.⁴⁸ This protection includes a protected disclosure to the DNI (or any employees designated by the DNI for such purpose), the ICIG, the head of the employing agency (or an employee designated by the head of that agency for such purpose), or the appropriate inspector general of the employing agency. Moreover, Section 601, unlike PPD-19, explicitly allows protected disclosures to be made to “a

⁴⁶ The Directive pertains to all elements of the IC except the Federal Bureau of Investigation (FBI). See PPD-19 Para C.

⁴⁷ The provisions under this legislation cover all IC elements *except* the Intelligence Branch of the Federal Bureau of Investigation (FBI/IB). See 50 U.S.C. §3234(a)(2)(B).

⁴⁸ The scope of personnel actions covered by Title VI includes an appointment, promotion, disciplinary or corrective action, detail, transfer, reassignment, demotion, suspension, termination, reinstatement or restoration, a performance evaluation, a decision concerning pay, benefits or awards, a decision concerning education or training if such education or training may reasonably be expected to lead to an appointment, promotion, or performance evaluation, or any other significant change in duties, responsibilities or working conditions. See 50 U.S.C. §3234(a)(3).

congressional intelligence committee, or a member of a congressional intelligence committee....”⁴⁹ Section 601 Title VI makes no specific mention of related protections for contractors.

A protected disclosure is defined as a disclosure that an IC employee whistleblower reasonably believes evidences a violation of “Federal law, rule or regulation ... or mismanagement, a gross waste of funds, an abuse of authority, or substantial and specific danger to public health and safety.”⁵⁰

Section 602 of Title VI provides protections against retaliatory revocation of the security clearance of a covered government employee whistleblower for making a protected disclosure.⁵¹ It also requires the development of *appeal* policies and procedures for any decision affecting a whistleblower’s security clearance that the whistleblower alleges is in reprisal for having made a protected disclosure. This provision also enables the whistleblower to retain his/her current employment status in the government, pending the outcome of the appeal.⁵² The law does not permit judicial review, nor does it provide a private right of action.⁵³ Like Section 601, Section 602 of Title VI does not describe protections for contractors.

Intelligence Community Directive (ICD)-120

First signed in 2014, and updated on April 29, 2016, ICD-120, *Intelligence Community Whistleblower Protection*, provides IC implementing guidance for PPD-19.⁵⁴ ICD-120 provides protections against reprisals involving (1) personnel actions (as defined by PPD), and (2) access to classified information. ICD-120 protections involving personnel actions do not apply to members of the Armed Forces or contractors. The protections governing access to classified information, however, do apply to both contractors and members of the Armed Forces. ICD-120 provisions include the following:

- protections from reprisal involving a personnel action against the IC employee making a protected disclosure.⁵⁵
- protections from reprisal for a protected disclosure that could affect an IC whistleblower’s eligibility for access to classified information.⁵⁶

⁴⁹ 50 U.S.C. §3234(b). The April 29, 2016, update to ICD-120 conformed with this section by also allowing protected disclosures to be made to the congressional intelligence committees or their Members.

⁵⁰ Section 601(b)(1)-(2) of P.L. 113-126, codified in 50 U.S.C. §3234(b)(1)(A)-(B).

⁵¹ Section 602 protections against the revocation of security clearances, codified as 50 U.S.C. §3341(j), applies to all elements of the IC—including the FBI/IB—in addition to other Executive Branch departments and agencies. It makes no mention of members of the Armed Forces who might be assigned to an IC element.

⁵² 50 U.S.C. §3341(b)(7)(A).

⁵³ A private right of action would permit an individual to bring a lawsuit.

⁵⁴ Intelligence Community Directive (ICD)-120, *Intelligence Community Whistleblower Protection*, at <https://www.odni.gov/files/ICIG/Documents/Hotline/Legal%20Docs/Intelligence%20Community%20Whistleblower%20Protection.pdf>.

⁵⁵ The ICD-120 provision protecting against personnel actions made in retaliation for a protected disclosure covers all elements of the IC with the specific exception of the FBI. See ICD-120(E)(1)(d), at <https://www.dni.gov/files/documents/ICD/ICD-120-IC-Whistleblower-Protection-2016-04-29.pdf>.

⁵⁶ “Employee” is defined to include a person “employed by, detailed or assigned to” an IC element including members of the Armed Forces, an expert or consultant to an agency, a contractor, licensee, certificate holder or grantee of an agency, or personal services contractor, or “any other category of person who acts for or on behalf of an agency as determined by the appropriate agency head.” See ICD-120(F)(1)(b)(1).

- a requirement for each IC element to have a review process to permit appeals for any decision involving a security clearance allegedly in retribution for making a protected disclosure.⁵⁷
- provision for an employee alleging a reprisal who has exhausted the internal agency review process to request an External Review Panel chaired by the ICIG.⁵⁸
- a requirement for IC-wide communications and training on whistleblower protections.⁵⁹
- a provision for an ICIG-chaired External Review Panel, consistent with the provision for such a panel in PPD-19.⁶⁰

Whistleblower Protections for Members of the Armed Forces Assigned to the IC

Section 1034 of Title 10, U.S. Code, provides protections against personnel actions taken in retaliation for protected communications by members of the Armed Forces.⁶¹ The Office of the DNI cites this statute as applicable to members of the Armed Forces assigned to the IC elements.⁶² Section 1034—unlike the ICWPA, which makes no mention of its applicability to the Armed Forces—does not provide a process for making a protected communication that also protects classified information. Section 1034

- allows members of the Armed Forces to communicate with a Member or Members of Congress; an Inspector General;⁶³ a member of a DOD audit, inspection, investigation, or law enforcement organization; any person or organization in the chain of command; a court-martial proceeding; or any other organization designated pursuant to regulations or other established administrative procedures for such communications;
- allows members of the Armed Forces to testify or otherwise participate or assist in an investigation or proceeding involving Congress or an Inspector General;
- specifies prohibited personnel actions in reprisal for a member of the Armed Forces making a protected communication;⁶⁴

⁵⁷ ICD-120(F)(1)(a). In addition, 50 U.S.C. §3341(b)(7)(A) provides for a whistleblower to maintain his/her employment status while a decision on an appeal is pending. Specifically, this provision requires the Executive Branch to develop policy and procedures “that permit, to the extent practicable, individuals alleging reprisal for having made a protected disclosure (provided the individual does not disclose classified information or other information contrary to law) to appeal any action affecting an employee’s access to classified information and *to retain their government employment status while such challenge is pending.*” [emphasis added]

⁵⁸ ICD-120(G)(1)(a).

⁵⁹ ICD-120(D)(1)(a).

⁶⁰ ICD-120(G).

⁶¹ This statute uses the term *communication* instead of *disclosure*.

⁶² See “Military Whistleblower Protections” at the Office of the Director of National Intelligence, “What Are My Protections?” at <https://www.dni.gov/ICIG-Whistleblower/protected.html>. See also DOD Directive 7050.06, *Military Whistleblower Protection*, April 17, 2015 at https://www.dodig.mil/Portals/48/Documents/Policy/DoDD_7050_06.pdf.

⁶³ 10 U.S.C. §1034(a)(1) provides that no person may restrict a member of the Armed Forces from making a protected communication to a Member of Congress or to an Inspector General.

⁶⁴ 10 U.S.C. §1034(b)(2)(A) states the following:

(continued...)

- enables the DOD to take action to mitigate hardship for an Armed Forces member following a preliminary finding concerning an alleged reprisal for a protected communication;⁶⁵
- requires the inspector general conducting an investigation into a protected communication to provide periodic updates to the whistleblower, the Secretary of Defense, and the relevant service;⁶⁶ and
- requires the DOD Inspector General to prescribe uniform standards for (1) investigations of allegations of prohibited personnel actions, and (2) training for staffs of Inspectors General on the conduct of such investigations.⁶⁷

Legislation to Address Perceived Gaps in Protections for IC Contractors

Originally, IC whistleblower legislation did not cover contractors. To address this perceived gap, Congress included in P.L. 115-118, the Foreign Intelligence Surveillance Reauthorization Act of 2017, protections for contractors similar to those for IC federal employees under Title VI of the IAA for FY2014 (P.L. 113-126).

Congress, through Section 110 of P.L. 115-118, titled “Whistleblower Protections for Contractors of the Intelligence Community,” enabled IC contractors to make disclosures while being protected against any retaliatory personnel action or retaliatory revocation of security clearances.⁶⁸

These protections extend to contractors of the FBI—including contractors of the IC element of the FBI, the Intelligence Branch—similar to the protections for IC employees and contractors under Section 3234 of Title 50, U.S. Code, as amended.⁶⁹

The actions considered for purposes of this section to be a personnel action prohibited by this subsection shall include any action prohibited by paragraph (1), including any of the following:

- (i) The threat to take any unfavorable action.
- (ii) The withholding, or threat to withhold, any favorable action.
- (iii) The making of, or threat to make, a significant change in the duties or responsibilities of a member of the armed forces not commensurate with the member’s grade.
- (iv) The failure of a superior to respond to any retaliatory action or harassment (of which the superior had actual knowledge) taken by one or more subordinates against a member.
- (v) The conducting of a retaliatory investigation of a member.

⁶⁵ 10 U.S.C. §1034(c)(4)(E).

⁶⁶ 10 U.S.C. §1034(e)(3)(A).

⁶⁷ 10 U.S.C. §1034, note (“Uniform Standards for Inspector General Investigations of Prohibited Personnel Actions and Other Matters”). The National Defense Authorization Act (NDAA) for Fiscal Year 2017 also required the Comptroller General of the United States to review the integrity of the DOD whistleblower protection program and report to the Senate and House Armed Services Committees no later than 18 months after the date of enactment of the NDAA on whether the program satisfies Executive Branch whistleblower protection policy. See P.L. 114-328, §536(a)-(b). Department of Defense (DOD) implementing guidance for 10 U.S.C. §1034 can be found in DOD Directive 7050.06, *Military Whistleblower Protection*. For more on whistleblower protections for the military, see CRS In Focus IF11499, *Protecting Military Whistleblowers: 10 U.S.C. §1034*, by Alan Ott.

⁶⁸ P.L. 115-118, §110, codified in 50 U.S.C. §3234(c).

⁶⁹ See P.L. 115-118, §110(b)(1)-(5).

Issues Raised by the IC Whistleblower Complaint of August 2019

The August 2019 whistleblower complaint (hereafter referred to as the 2019 whistleblowing complaint) that led to the first impeachment of President Trump highlighted some differences in how officials responsible for handling IC complaints interpret existing IC whistleblowing statutes.

The complaint concerned the July 25, 2019, phone call between President Trump and Ukrainian President Volodymyr Zelensky during which, the complainant alleged, President Trump pressured the Ukrainian president to initiate an investigation into then-presidential candidate Joseph R. Biden and his son. According to allegations, President Trump hoped the investigation would enhance his prospects for reelection.⁷⁰

The ICIG who received the complaint determined within 14 days, as required by the whistleblowing statute, that it appeared credible and was a matter of urgent concern.⁷¹ The ICIG supported his determination in a statement in which he indicated that the President's phone call fell within the scope of what constituted the "funding, administration, or operation of an intelligence activity within the responsibility and authority of the Director of National Intelligence." Specifically, the ICIG cited the establishment of the IC Election Threats Executive position on July 19, 2019, and then-DNI Daniel Coats' statement that "Election security is an enduring challenge and a top priority for the IC."⁷² The ICIG cited as well the relevant sections of two executive orders (E.O.):

- Section 1.4 of E.O. 12333, *United States Intelligence Activities*, which states that the IC "under the leadership of the Director [of National Intelligence]" shall "collect information concerning and conduct activities to protect against ... intelligence activities directed against the United States."⁷³
- E.O. 13848, *Imposing Certain Sanctions in the Event of Foreign Interference in a United States Election*, which states in part, "[T]he ability of persons located, in whole or in part, outside of the United States to interfere in or undermine public confidence in United States elections ... constitutes an unusual and extraordinary threat to the national security and foreign policy of the United States."⁷⁴

Upon receiving the complaint from the ICIG, the acting DNI sought the advice of the White House Counsel's Office on whether the phone call between President Trump and the Ukrainian president was subject to executive privilege.⁷⁵ According to the acting DNI's congressional

⁷⁰ Zachary B. Wolf and Sean O'Key, "Trump-Ukraine Impeachment Inquiry Report, Annotated," *CNN*, December 3, 2019, at <https://www.cnn.com/interactive/2019/12/politics/trump-ukraine-impeachment-inquiry-report-annotated/>.

⁷¹ *Office of the Inspector General of the Intelligence Community Michael Atkinson Letter to the Acting Director of National Intelligence Joseph Maguire*, August 26, 2019, p. 5, at <https://www.documentcloud.org/documents/6442986-National-Security-Archive-Doc-05-Temporary>. The relevant statute is 50 U.S.C. §3033(k)(5)(B).

⁷² Quoted from *Letter from the Inspector General of the Intelligence Community, Michael Atkinson, to the Acting Director of National Intelligence, Joseph Maguire*, August 26, 2019, p. 5 at <https://assets.documentcloud.org/documents/6430413/IG-Letter-Ukraine-Whistleblower.pdf>.

⁷³ *Ibid.*, p. 4.

⁷⁴ *Ibid.* For E.O. 13848, see <https://www.federalregister.gov/documents/2018/09/14/2018-20203/imposing-certain-sanctions-in-the-event-of-foreign-interference-in-a-united-states-election>.

⁷⁵ See *Opening Statement by Acting Director of National Intelligence Joseph Maguire before the House Permanent* (continued...)

testimony, the White House Counsel's Office replied that much of it was. The acting DNI, therefore, determined that DNI was unable to forward the complaint to Congress within seven days of receiving it, as would have been required for typical complaints governed by the IC whistleblowing statutes.⁷⁶

On September 3, 2019, the Department of Justice Office of Legal Counsel (OLC), responding to a request by the General Counsel of the IC, issued an opinion on the complaint.⁷⁷ The opinion outlined two fundamental differences with the ICIG:

- that the complaint did not constitute a matter of “urgent concern” since the ICIG whistleblower statute, 50 U.S.C. §3033, was not applicable as the complaint involved the President and not a member of the IC; and
- that the complaint was unrelated to “the funding, administration, or operation of an intelligence activity under the authority of the Director of National Intelligence.”⁷⁸ The OLC suggested that, since the alleged wrongdoing did not involve an intelligence activity, it fell outside the responsibility of the ICIG to investigate the complaint's credibility.⁷⁹

It was the opinion of the OLC, therefore, that the DNI was not statutorily obligated to forward the complaint to the congressional intelligence committees as would have been required under 50 U.S.C. §3033(k)(5)(C). The OLC opinion stated that while the ICIG whistleblower statute covers activities of an urgent concern within the IC, “this provision ... does not cover every alleged violation of federal law or other abuse that comes to the attention of a member of the intelligence community.”⁸⁰ Accordingly, the OLC referred the complaint to the DOJ's Criminal Division for review of possible campaign finance violations in accordance with 28 U.S.C. §535(b) (“Investigation of Crimes Involving Government Officers and Employees”).⁸¹

In a September 6, 2019, letter to the Chair and Ranking Member of the House Permanent Select Committee on Intelligence, the then-ICIG, Michael Atkinson, stated that the acting DNI's decision not to forward the complaint within seven days was a departure from past practice where even complaints that were deemed not to be matters of urgent concern were forwarded.⁸² The

Select Committee on Intelligence, September 26, 2019, at <https://www.dni.gov/index.php/newsroom/congressional-testimonies/item/2048-acting-dni-opening-statement>. See also acting Director Maguire's complete testimony at <https://www.c-span.org/video/?464509-1/acting-director-national-intelligence-maguire-testifies-whistleblower-complaint>.

⁷⁶ *Ibid.*

⁷⁷ See Steven A. Engel, Assistant Attorney General Office of Legal Counsel, *Memorandum of Opinion for the General Counsel Office of the Director of National Intelligence*, September 3, 2019, at <https://www.justice.gov/olc/opinion/file/1205711/download>.

⁷⁸ *Ibid.* The opinion cited the definition of “urgent concern” in 50 U.S.C. §3033(k)(5)(G)(i).

⁷⁹ *Ibid.*, p. 10.

⁸⁰ *Ibid.*, p. 5.

⁸¹ *Ibid.*, p. 2. The DOJ indicated the Criminal Division terminated its investigation in September 2019 after making a determination that no campaign finance violation had occurred. See Matt Zapotosky and Devlin Barrett, “Justice Department Rejected Investigation of Trump Phone Call Just Weeks After It Began Examining the Matter,” *Washington Post*, September 25, 2019, at https://www.washingtonpost.com/national-security/justice-dept-rejected-investigation-of-trump-phone-call-just-weeks-after-it-began-examining-the-matter/2019/09/25/6f7977ce-dfb5-11e9-8dc8-498eabc129a0_story.html.

⁸² In his September 26, 2019, testimony before the House Permanent Select Committee on Intelligence, Acting DNI Maguire acknowledged that his not forwarding the complaint to Congress within seven days as required by the IC whistleblowing statutes was a departure from past practice. He cited the “unprecedented” circumstances that he believed prevented him from doing so. See *Opening Statement by Acting Director of National Intelligence Joseph* (continued...)

acting DNI's decision enabled the complainant to contact the committees directly "in an authorized and protected manner."⁸³

The acting DNI forwarded the complaint to Congress on September 25, 2019, once the Trump Administration released what was described as a transcript of President Trump's phone call.⁸⁴

117th Congress: Intelligence Authorization Act for Fiscal Year 2022

The Intelligence Authorization Act for Fiscal Year 2022 (Division X of the Consolidated Appropriations Act for Fiscal Year 2022 (P.L. 117-103) (IAA for FY2022) included several provisions to address inconsistent language in the different intelligence community whistleblowing statutes, add clarity to the process for making a protected disclosure, and underscore the independence of inspectors general.

Selected Provisions

Harmonization of Language

The IAA for FY2022 amended whistleblower provisions in Title 50, United States Code, to help ensure consistency (or "harmonization") in the text of IC-related whistleblower statutes. Among the changes, the IAA for FY 2022:

- Amended Title 50 prohibited personnel practices to make the text consistent with the text of prohibitions in PPD-19 and Section 101 of the Civil Service Reform Act of 1978 (P.L. 95-454).⁸⁵ As amended, Title 50 prohibited personnel practices now include an IC employer making a *threat* of a reprisal against an IC employee or contractor who makes a protected disclosure that the individual "reasonably believes" provides evidence of a violation of the law, rule or regulation; or of mismanagement, a waste of funds, abuse of authority, or a danger to public health and safety;⁸⁶

Maguire before the House Permanent Select Committee on Intelligence, September 26, 2019, at <https://www.dni.gov/index.php/newsroom/congressional-testimonies/item/2048-acting-dni-opening-statement>. See also acting Director Maguire's complete testimony at <https://www.c-span.org/video/?464509-1/acting-director-national-intelligence-maguire-testifies-whistleblower-complaint>.

⁸³ See *Inspector General of the Intelligence Community Michael Atkinson Letter to the Honorable Adam Schiff, Chairman, and the Honorable Devin Nunes, Ranking Member, of the Permanent Select Committee on Intelligence, House of Representatives*, September 6, 2019, at https://intelligence.house.gov/uploadedfiles/20190909_-_ic_ig_letter_to_hpsci_on_whistleblower.pdf:

The ICIG has on occasion in the past determined that, for a variety of reasons, disclosures submitted to the ICIG under the urgent concern statute did not constitute an urgent concern. In those cases ... the DNI nevertheless provided direction to the ICIG to transmit the ICIG determination and the complainant's information to the congressional intelligence committees.... That past practice permitted complainants in the Intelligence Community to contact the congressional intelligence committees directly, in an authorized and protected manner, as intended by the urgent concern statute. (p. 2)

⁸⁴ *Opening Statement by Acting Director of National Intelligence Joseph Maguire before the House Permanent Select Committee on Intelligence*, September 26, 2019, at <https://www.dni.gov/index.php/newsroom/congressional-testimonies/item/2048-acting-dni-opening-statement>. See also Admiral Maguire's complete testimony at <https://www.c-span.org/video/?464509-1/acting-director-national-intelligence-maguire-testifies-whistleblower-complaint>.

⁸⁵ The relevant provisions of P.L. 95-454, §101 are codified at 5 U.S.C. §2302(b)(8).

⁸⁶ This provision of P.L. 117-103 amended 50 U.S.C. §3234(b) and (c)(1), pertaining to IC element employees and (continued...)

- Amended Title 50 prohibited personnel practices by specifying that the President enforce prohibitions against reprisals (including the revocation of security clearances) for a whistleblower making a protected disclosure “consistent ... with the policies and procedures used to adjudicate alleged violations” of an employee or contractor’s right to make a protected disclosure as referenced in the Civil Service Reform Act of 1978;⁸⁷ and
- Established consistency with respect to language: In two provisions describing the basis for making a protected disclosure, the qualifier “gross mismanagement” is simplified to “mismanagement” to ensure consistency with the use of “mismanagement” in other IC whistleblowing-related statutes.⁸⁸
- Codified in 50 U.S.C. §3236 the external review panels that were initially established in PPD-19 and ICD-120.

Employee Rights Concerning Security Clearance Decisions

The IAA for FY2022 amended Title 50 provisions governing intelligence element decisions to revoke security clearances. The amended provisions allow for the tolling (or delaying) of the 90-day time limit for an employee to appeal an IC element eligibility decision if the employee provides “substantial credible evidence” as to why the employee did not timely initiate the appeal and why enforcement of the time limit would be unfair.⁸⁹

Officials Authorized to Receive a Protected Disclosure

The IAA for FY2022 amended provisions governing recipients of a protected disclosure by adding language that an employee can make a protected disclosure to a supervisor in the employee’s direct chain of command, or a supervisor of the employing or contracting agency up to and including the head of the employing or contracting agency.⁹⁰

Independence of Inspectors General

The IAA for FY2022 amended provisions governing IC whistleblowing adjudication by specifically designating the ICIIG or Inspector General of the IC element to whom a whistleblower makes a complaint as “having sole authority to determine whether a complaint or information ... is a matter of urgent concern....”⁹¹

Issues for Congress

An IC whistleblower, by definition, is someone who reports to an appropriate authority, in a manner that protects classified information, a matter the whistleblower reasonably believes to be a serious wrongdoing, flagrant abuse, or a violation of law involving an intelligence activity. A retrospective review of IC whistleblowing legislation, whether passed or not, generally appears to

contractors, respectively. It applies to all statutory IC elements except the FBI’s Intelligence Branch (IB). See 50 U.S.C. §3234(a)(1).

⁸⁷ Section 501 of Title V of the IAA for FY2022 amends 50 U.S.C. §§3234(d) and 3341(j) by aligning these statutes with enforcement policy and procedures referenced in the Civil Service Reform Act of 1978 (5 U.S.C. §2302(b)(8)).

⁸⁸ These amendments are to 50 U.S.C. §§3341(j)(1)(A)(ii), 3341(j)(1)(B)(ii), and 3234(c)(1)(B).

⁸⁹ 50 U.S.C. §3341(j)(4)(D).

⁹⁰ 50 U.S.C. §§3234(b), 3234(c)(1), 3341(j)(1)(A)(i).

⁹¹ 50 U.S.C. §§3033(k)(5)(G)(ii) and 3517(d)(5)(G)(ii); and 5 U.S.C. §416 note.

demonstrate congressional encouragement for potential whistleblowers to report on issues that otherwise may have limited means of oversight because of their classified nature. The circumstances of the 2019 whistleblowing incident that led to the first impeachment of President Donald J. Trump exposed a number of areas with the potential to stimulate discussion on whether existing law meets Congress’s intent to encourage whistleblowers to come forward. A number of these areas have been addressed in subsequent legislation, such as the provision in the IAA for FY2022 that gave the inspectors general of IC elements “sole authority” for determining whether a protected disclosure constitutes a matter of “urgent concern.” In addition, the House Permanent Select Committee on Intelligence (HPSCI), in its version of the IAA for FY2022, considered provisions requiring training and an “Office of Victim and Whistleblower Counsel and Special Victim Investigator” at the CIA to assist whistleblowers who report allegations of sexual harassment and related misconduct.⁹² This came in the aftermath of whistleblower reports of sexual assault at the agency.⁹³ Congress may consider legislation following up on these remaining issues centered on the following questions:

- Should whistleblowers have a right to remain anonymous? If so, what, if any, recourse do they have in the event their identity is disclosed against their will? How would a whistleblower’s anonymity affect the rights and response of the accused?
- Are the procedures for making disclosures, including disclosures to Congress, clear, and do they provide for the protection of classified information?
- If Congress were to consider legislation requiring IC elements to institute training on appropriate responses to allegations of sexual harassment and related misconduct, should the legislation include support for victim’s reporting allegations?

Author Information

Michael E. DeVine
Analyst in Intelligence and National Security

⁹² Section 801 of Title VIII of H.R. 3932, the Intelligence Authorization Act for Fiscal Year 2024.

⁹³ See, for example, Daniel Lippman, “House Intel Committee Pushing New Legislation to Help CIA Sexual Assault Victims,” *Politico*, July 13, 2023, at <https://www.politico.com/news/2023/07/13/house-intel-committee-pushing-new-legislation-to-help-cia-sexual-assault-victims-00106104>.

Disclaimer

This document was prepared by the Congressional Research Service (CRS). CRS serves as nonpartisan shared staff to congressional committees and Members of Congress. It operates solely at the behest of and under the direction of Congress. Information in a CRS Report should not be relied upon for purposes other than public understanding of information that has been provided by CRS to Members of Congress in connection with CRS's institutional role. CRS Reports, as a work of the United States Government, are not subject to copyright protection in the United States. Any CRS Report may be reproduced and distributed in its entirety without permission from CRS. However, as a CRS Report may include copyrighted images or material from a third party, you may need to obtain the permission of the copyright holder if you wish to copy or otherwise use copyrighted material.