

Intelligence Community Whistleblower Protections

Updated June 22, 2021

Congressional Research Service

<https://crsreports.congress.gov>

R45345



R45345

June 22, 2021

Michael E. DeVine

Analyst in Intelligence and
National Security

Intelligence Community Whistleblower Protections

Intelligence community (IC) whistleblowers are those employees or contractors 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 are publicly available and specifically 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 many observers believed left 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 only 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 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 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) the clarity of procedures on how to make a lawful disclosure; (2) policy and process enabling a whistleblower to approach Congress directly; (3) the degree of independence of IC inspectors general to make final determinations specific to a complaint; (4) the jurisdiction of an IC inspector general to handle a complaint—whether it can concern a subject who is not a member of an IC element, or conduct that is not unambiguously connected to an intelligence activity; and (5) the adequacy of protections against unlawful disclosure of a whistleblower's identity.

This report traces the evolution of IC whistleblower protections in legislation and presidential and IC directives. Effective whistleblowing protections are considered as much about instilling confidence in the integrity and comprehensiveness of the process for submitting a complaint as they are about the process itself. When IC employees have confidence they can make protected disclosures anonymously and without fear of retribution, they are often more likely to adhere to a process that is also intended to protect classified information. Conversely, a lack of confidence can increase the chances of wrongdoing going unreported or classified information being compromised through an employee's making a complaint outside of proper channels.

Contents

Introduction	1
Evolution of Whistleblower Protection Laws and Policy.....	2
Intelligence Community Whistleblower Protection Act (ICWPA) of 1998	2
Intelligence Authorization Act (IAA) for Fiscal Year 2010	5
Presidential Policy Directive (PPD)-19.....	7
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
Resources to Enhance Whistleblower Investigations.....	13
Issues Raised by the IC Whistleblower Complaint of August 2019.....	13
Proposed IC Whistleblower Legislation, 116 th Congress	16
S. 3905, Intelligence Authorization Act (IAA) for Fiscal Year 2021 (Introduced)	16
Protection of a whistleblower’s identity from disclosure	16
Greater latitude for a whistleblower to report directly to Congress.....	16
Expanded definition of “urgent concern”	17
Independence of the ICIG	17
H.R. 7856, Intelligence Authorization Act for Fiscal Year 2021 (Introduced).....	17
Protection of a whistleblower’s identity from disclosure	17
Greater latitude for a whistleblower to report directly to Congress.....	17
Expansion of the definition of “urgent concern”	18
Independence of IC Element Inspectors General.....	18
Expansion of the responsibilities of the DNI	18
Potential Questions for Congress	18

Contacts

Author Information.....	19
-------------------------	----

Introduction

Intelligence Community (IC) whistleblowers are those employees or contractors working in any of the statutory elements of the IC who disclose their reasonable beliefs 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 essential 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. The Director of National Intelligence (DNI) whistleblowing policy and guidance are publicly available and specifically address whistleblower process and protections for IC contractors, members of the Armed Forces, and federal employees.² There are differing opinions, however, on whether the IC's internal processes are entirely clear and have the transparency necessary, from the standpoint of a whistleblower, to ensure adequate protections against reprisal.

Whistleblower protections for employees and contractors in the IC are extended only to those who make a lawful disclosure. They do not cover disclosures that do not conform to statutes and directives prescribing reporting procedures intended to protect classified information, for example, by classified information disclosures to the media or a foreign government. The whistleblower protections do not apply to a difference of opinion over policy, strategy, analysis, or priorities for intelligence funding or collection, unless there is a reasonable concern over legality or constitutionality. Whistleblower protections also do not protect against legitimate adverse personnel or security clearance eligibility decisions if the agency can demonstrate that it would have taken the same action in the absence of a protected disclosure.

IC whistleblower protections have evolved in response to perceptions of gaps that many believed left whistleblowers vulnerable to reprisal. The first whistleblower legislation specific to the IC was the Intelligence Community Whistleblower Protection Act (ICWPA) of 1998. It was limited to specifying a process for an IC whistleblower to make a complaint but offered no specific protections. The Intelligence Authorization Act for Fiscal Year 2010 included provisions for protecting IC whistleblowers, though these were general and subject to different standards of implementation.

Presidential Policy Directive (PPD)-19, signed in 2012, provided the first specific protections in response to perceptions that IC whistleblowers remained vulnerable to reprisal actions for making a complaint. The Intelligence Authorization Act for Fiscal Year 2014 codified the PPD-19 provisions (50 U.S.C. §§3231 et seq.), and Intelligence Community Directive (ICD)-120 established a PPD-19 implementation policy. 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*. The most recent legislation concerning IC whistleblowers was Section 110 of P.L. 115-118, enacted in January 2018, which amended the National Security Act of 1947 and the Intelligence Reform and Terrorism Prevention Act of 2004 to include provisions to address perceived gaps in protections for IC contractors.

¹ <https://www.dni.gov/ICIG-Whistleblower/index.html>.

² <https://www.dni.gov/ICIG-Whistleblower/process-how.html>.

The August 2019 whistleblower complaint that led to the impeachment of President Donald J. Trump revealed a number of differences in how IC whistleblowing statutes could be interpreted. There were differences over the jurisdiction of an IC inspector general to handle complaints concerning individuals outside the IC whose conduct is not unequivocally related to an intelligence activity and the independence of IC inspectors general to make a final determination of whether a complaint is credible and a matter of “urgent concern.” In addition, there were differences over whether the statute should provide comprehensive protections against disclosure of a whistleblower’s identity.

IC whistleblower laws are codified in four separate statutes: the Inspector General Act of 1978, as amended (5 U.S.C. App. §8H), that applies to the inspectors general of all IC elements; the Central Intelligence Agency (CIA) Act of 1949, as amended (50 U.S.C. §3517), that applies to the inspector general of the CIA; the National Security Act of 1947, as amended (50 U.S.C. §3033), that applies to the ICIG, and Title VI of the Intelligence Authorization Act for Fiscal Year 2014, as amended (50 U.S.C. §3234) that provides protections for whistleblowers making a lawful disclosure.

Evolution of Whistleblower Protection Laws and Policy

Intelligence Community Whistleblower Protection Act (ICWPA) of 1998

The Intelligence Community Whistleblower Protection Act of 1998 (ICWPA),³ as amended, is intended to assist whistleblowers in the IC who are specifically excluded from the Whistleblower Protection Act of 1989, which applies to federal employees outside of the IC who work in an unclassified environment. The ICWPA makes no provision for members of the Armed Forces assigned to an IC element.⁴ The act amended the CIA Act of 1949 and the Inspector General Act of 1978 to enable an IC government 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 involving classified information, but does not include differences of opinions concerning public policy matters;⁵

³ Title VII of the Intelligence Authorization Act for Fiscal Year 1999, P.L. 105-272, §§701-702, codified in 5 U.S.C. App. §8H, 50 U.S.C. §3033, and 50 U.S.C. §3517.

⁴ 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.

⁵ 5 U.S.C. §8H(h)(1)(A-C), 50 U.S.C. §3517(d)(5)(G)(i)(I), and 50 U.S.C. §3033(k)(5)(G)(i) provide definitions for “urgent concern,” as the term relates to the Intelligence Community. The ICWPA of 1998 definition for “urgent concern” (noted above) is codified in 50 U.S.C. §3517(d)(5)(G)(i)(I), *Inspector General of the CIA*, as well as in 5 U.S.C. App. §8H(1), *Additional Provisions with Respect to Inspectors General of the Intelligence Community*. The Intelligence Authorization Act for 2010 (P.L. 111-256) that created the position of Inspector General of the Intelligence Community, codified in 50 U.S.C. §3033(k)(5)(G)(i), *Inspector General of the Intelligence Community*, differs in its definition only in its reference to the DNI’s authority. An “urgent concern” is:

(B) a false statement to the Congress, or a willful withholding from Congress of an issue of material fact relating to the funding, administration, or operation of an intelligence activity;⁶ or

(C) an action ... constituting reprisal or threat of reprisal ... in response to an employee's reporting of an urgent concern.⁷

Congress noted that the absence of a statutory IC whistleblower protection mechanism previously “may have impaired the flow of information needed by the intelligence committees to carry out oversight responsibilities.”⁸ Consequently, the ICWPA of 1998 defines the formal processes for submitting complaints to ensure the protection of any classified information:⁹

- A designee of the IG who receives a complaint of an urgent concern from an employee has 7 days from receipt to report the complaint to the intelligence element's IG.¹⁰
- 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.¹¹
- Within 7 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.¹²

A serious or flagrant problem, abuse, violation of law or executive order, or deficiency relating to the funding, administration, or operation of an intelligence activity *within the responsibility and authority of the Director of National Intelligence* involving classified information, but does not include difference of opinions concerning public policy matters. [emphasis added]

This distinction became important in the September 26, 2019, opinion of the Department of Justice (DOJ) Office of Legal Counsel (OLC), concerning the whistleblowing complaint directed at President Trump. The OLC cited the 50 U.S.C. §3033(k)(5)(G)(i) definition to support its opinion that President Trump's phone call to the Ukrainian president on July 25, 2019, was not a matter of urgent concern since it did not constitute “an intelligence activity within the responsibility and authority of the Director of National Intelligence.” Although the whistleblower and ICIG invoked only 50 U.S.C. §3033(k)(5)(G)(i), the OLC opinion also maintained that the 5 U.S.C. App. §8H definition was applicable: “The definition of “urgent concern” in the IG Act is not limited to intelligence activities that are specifically “within the responsibility and authority of the” DNI because the complaint procedures in section 8H are written to apply to multiple inspectors general within the intelligence community.” See *Memorandum for Jason Klitenic, General Counsel Office of the Director of National Intelligence, from Steven A. Engel, Assistant Attorney General, Office of Legal Counsel*, September 24, 2019, p. 6, at <https://www.justice.gov/olc/opinion/file/1205711/download>.

⁶ 5 U.S.C. §8H(h)(i)(1)(B), 50 U.S.C. §3033(k)(5)(G)(ii), 50 U.S.C. §3517(d)(5)(G)(i)(II).

⁷ 5 U.S.C. §8H(h)(i)(1)(C), 50 U.S.C. §3033(k)(5)(G)(iii), 50 U.S.C. §3517(d)(5)(G)(i)(III).

⁸ P.L. 105-272, §701.

⁹ The process for submitting a whistleblower complaint in the IC is provided in 5 U.S.C. App. §8H and 50 U.S.C. §3033(k).

¹⁰ 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. App. §8H(a)(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. App. §8H(h).

¹¹ 50 U.S.C. §3033(k)(5)(B), 5 U.S.C. App. §8h(b)(1), 50 U.S.C. §3517(d)(5)(B)(i).

¹² Section 7(b) of the Inspector General Act of 1978 (5 U.S.C. App.) 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.

- 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.¹³
- 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.
- 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.
- The intelligence element's IG will notify the employee making the complaint of any action involving the complaint within 3 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.

Although the ICWPA provides a process for IC whistleblowers—employees and contractors—to securely report complaints to Congress via the IG of the whistleblower's IC agency, it offers no specific provisions for protecting whistleblowers from reprisal or punishment. Subsequent

The whistleblowing provision pertaining to the ICIG, 50 U.S.C. §3033(k)(5), 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.)." These measures, however, are not applicable to anyone other than the inspector general handling a complaint. They do not afford protections against disclosure by someone other than the inspector general, such as a member of the media or a Member of Congress if they 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) an IG determination that disclosure is "unavoidable" in the course of the investigation; or (2) when disclosure is to a Department of Justice official "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*," the Freedom of Information Act (FOIA). Subsection (b)(3) states that FOIA's mandatory disclosure requirements do not apply to covered materials "specifically exempted from disclosure by statute" in specified circumstances. The §3033 provision obligates an IC inspector general to protect a whistleblower's identity from disclosure under FOIA. For more information on FOIA, see 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 Intelligence Officers, Agents, Informants, and Sources*). This provision also includes an exception for disclosure to Congress.

¹³ The four DOD intelligence agencies are the National Security Agency, the National Reconnaissance Office, the National Geospatial-Intelligence Agency, and the Defense Intelligence Agency.

legislation that specifically prohibits actions taken in reprisal for an IC employee making a lawful disclosure (a disclosure that adheres to the 1998 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.¹⁴ Informing Congress was not contingent only upon the appropriate authority deciding a complaint constituted a “matter of urgent concern.” In the event the relevant IC element determines the complaint does not constitute a matter of urgent concern, the statute provides a process for a complainant to inform the congressional intelligence committees in any event.¹⁵

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.”¹⁶ They acknowledge that “the risk of reprisal perceived by employees and contractors of the Intelligence Community for reporting serious or flagrant problems to Congress may have impaired the flow of information needed by the intelligence committees to carry out oversight responsibilities.”¹⁷ In other words, Congress wanted to establish a means for a member of the IC to report allegations of wrongdoing, whether or not they were determined to be matters of urgent concern, so long as the process allowed for the protection of classified information.

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 Intelligence Community Inspector General (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. Section 3033 permits lawful disclosures to the ICIG and echoes the ICWPA’s provision protecting the whistleblower’s identity from disclosure, but otherwise it 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.¹⁸

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

¹⁴ P.L. 105-272§701(b)(6).

¹⁵ Section 701(b)(6) of H.Rept. 105-780, *Conference Report for the Intelligence Authorization Act for Fiscal Year 1999*.

¹⁶ P.L. 105-272 §701(b)(3).

¹⁷ P.L. 105-272 §701(b)(5).

¹⁸ 50 U.S.C. §3033(g)(3).

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”);¹⁹

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.²⁰

Section 3033 does cover contractors in addition to federal employees of IC elements:

An employee of an element of the intelligence community, an employee assigned or detailed to an element of the intelligence community, or an employee of a contractor to the intelligence community who intends to report to Congress a complaint or information with respect to an urgent concern may report such complaint or information to the Inspector General.²¹

Section 425(d) of the IAA for FY2010 also amended the CIA Act of 1949 to clarify existing protections against reprisals involving CIA employees who make lawful disclosures to the CIA Inspector General.²²

Finally, the FY2010 IAA provides a means for addressing differences that may arise between the ICIG and the DNI. Specifically,

- Section 3033 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.” In such situations, the DNI must submit to the congressional intelligence committees within seven days of his determination a statement explaining the reasons. The DNI must provide a copy to the ICIG who then may submit comments on the statement to the congressional intelligence committees.²³
- The ICIG shall “immediately notify, and submit a report to the congressional intelligence committees:”²⁴

¹⁹ 50 U.S.C. §3033(g)(3)(A).

²⁰ 50 U.S.C. §3033(g)(3)(B).

²¹ 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.”

²² P.L. 111-259, §425(d). The provisions for prohibiting reprisal actions for lawful whistleblower disclosures to the CIA Inspector General can be found in 50 U.S.C. §3517(e)(3)(A)-(B).

²³ 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>.

²⁴ 50 U.S.C. §3033(k)(3)(A). For the 2019 IC whistleblower complaint against President 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.dni.gov/index.php/newsroom/congressional-testimonies/item/2048-acting-dni-opening-statement>. See also

- in the event the DNI and ICIG cannot resolve a difference between them;²⁵
- the disagreement involves a matter involving an inspection, audit, or review of any current or former senior intelligence community official;²⁶ or
- the matter requires the ICIG to submit a report to the Department of Justice on possible criminal conduct by a senior intelligence official;²⁷ or
- the ICIG receives notice from the Department of Justice declining or approving prosecution of possible criminal conduct of any such official;²⁸ 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.²⁹
- 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.³⁰
- 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.³¹
- Although the IG has the authority to determine the credibility of a whistleblower complaint, the law does not specify who has the authority to determine whether a complaint, aside from its credibility, constitutes a matter of “urgent concern.”

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 protections for IC whistleblowers. PPD-19 specifically protects some employees in the IC—but specifically

Acting Director Maguire’s complete testimony 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>.

²⁵ 50 U.S.C. §3033(k)(3)(A)(i).

²⁶ 50 U.S.C. §3033(k)(3)(A)(ii) specifies intelligence officials subject to an audit, investigation, or inspection over which the DNI and ICIG might disagree, that 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 in an acting capacity.

²⁷ 50 U.S.C. §3033(k)(3)(A)(iii).

²⁸ 50 U.S.C. §3033(k)(3)(A)(iv).

²⁹ 50 U.S.C. §3033(k)(3)(A)(v).

³⁰ 50 U.S.C. §3033(k)(5)(I). This is limited to notification of the fact alone 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) and 5 U.S.C. App. §8H(d)(2).

³¹ 50 U.S.C. §3033(k)(4).

excludes members of the Armed Forces—with access to classified information, from personnel actions taken in reprisal for making a lawful disclosure.³²

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.³³

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.³⁴
- 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 lawful disclosure. The review process also must provide for the security of classified information involved in a disclosure.
- Requires, part of the review process, the IC element Inspector General to determine whether a personnel action was taken in reprisal for a lawful disclosure. The IG then may 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 lawful disclosures.

³² In addition to excluding members of the Armed Forces, 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 and leaked 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 of 1998, 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 (that 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.

³³ Presidential Policy Directive (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>.

³⁴ Adverse personnel actions might include demotion, transfer, termination, suspension, lower performance evaluation or punitive changes in duties and responsibilities.

- 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.³⁵

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

Title VI of the FY2014 IAA (P.L. 113-126), passed by Congress on July 7, 2014, codified provisions of PPD-19 (50 U.S.C. §3234) and provided the first expansive statutory protections for most IC whistleblowers against personnel or security clearance actions made in reprisal for protected disclosures.³⁶

- Section 601 of Title VI protects IC whistleblowers from any personnel action committed or omitted in retaliation for a lawful disclosure.³⁷ This includes a lawful 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), the appropriate inspector general of the employing agency, a congressional intelligence committee, or a Member of a congressional intelligence committee.³⁸
 - However, Section 601 of Title VI make no specific mention of related protections for contractors.
 - A lawful 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.”

³⁵ The Directive pertains to all elements of the IC except the Federal Bureau of Investigation (FBI). See PPD-19 Para F (3).

³⁶ 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).

³⁷ 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).

³⁸ Section 601 of P.L. 113-126 (50 U.S.C. §3234(b)), unlike PPD-19, explicitly allows protected disclosures to be made to “a congressional intelligence committee, or a member of a congressional intelligence committee....” 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.

- Section 602 of Title VI provides protections against retaliatory revocation of the security clearance of a covered government employee whistleblower for making a lawful disclosure.³⁹ 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.⁴⁰
 - Does not permit judicial review, nor does it provide a private right of action.⁴¹
 - Makes no specific mention of related 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. ICD-120 excludes personnel actions related to members of the Armed Forces, and makes no reference to contractors.⁴² ICD-120 provisions include the following:

- Protections against reprisal involving a personnel action against the IC employee making a protected disclosure.⁴³
- Protections from reprisal for a protected disclosure that could affect an IC whistleblower's eligibility for access to classified information.⁴⁴ This provision, which is specific to eligibility for access to classified information, applies to contractors and members of the Armed Forces.
- 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 lawful disclosure.⁴⁵

³⁹ 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.

⁴⁰ 50 U.S.C. §3341(b)(7).

⁴¹ A private right of action would permit an individual to bring a lawsuit.

⁴² See ICD-120(E)(1)(b)(4). Protections for members of the Armed Forces against personnel actions made in reprisal for a lawful disclosure are covered by 10 U.S.C. §1034. See below, "Whistleblower Protections for Members of the Armed Forces Assigned to the IC."

⁴³ The ICD-120 provision protecting against personnel actions made in retaliation for a lawful 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%20120%20-%20IC%20Whistleblower%20Protection%20\(29%20Apr%202016\).pdf](https://www.dni.gov/files/documents/ICD/ICD%20120%20-%20IC%20Whistleblower%20Protection%20(29%20Apr%202016).pdf).

⁴⁴ "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).

⁴⁵ 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

- 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.⁴⁶
- A requirement for IC-wide communications and training on whistleblower protections.⁴⁷

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.⁴⁸ The Office of the DNI cites this statute as applicable to members of the Armed Forces assigned to the IC elements.⁴⁹ 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;⁵⁰ 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;⁵¹

employment status while such challenge is pending.” [emphasis added]

⁴⁶ ICD-120(G)(1)(a).

⁴⁷ ICD-120(D)(1)(a).

⁴⁸ This statute uses the term *communication* instead of *disclosure*.

⁴⁹ See 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.

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

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

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.

- 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;⁵²
- requires the inspector general conducting an investigation into a protected communication to provide periodic updates to Congress, the whistleblower, the Secretary of Defense, and the relevant service;⁵³ 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.⁵⁴

Legislation to Address Perceived Gaps in Protections for IC Contractors

Efforts to cover contractors in IC whistleblower protection legislation has been inconsistent. The ICWPA of 1998, which provides a process for reporting a whistleblower complaint, does cover contractors, as do protections in Section 405 of the IAA for FY2010, and Title VI of the IAA of 2014.⁵⁵ Three subsequent efforts in Congress to address a perceived gap in coverage culminated on January 19, 2018, when Congress passed P.L. 115-118, the Foreign Intelligence Surveillance Reauthorization Act of 2017.

Section 110 of P.L. 115-118, titled “Whistleblower Protections for Contractors of the Intelligence Community,” amended Section 1104 of the National Security Act of 1947 by providing protections for IC contractor whistleblowers.⁵⁶ Section 110 amended existing whistleblower protections to enable IC *contractors* to make lawful disclosures to the head of the contracting agency (or an employee designated by the head of that agency for such purpose), or to the appropriate inspector general of the contracting agency, as well as to the DNI, ICIG, and the congressional intelligence committees (or Members of the committees). These protections are similar to those for IC employees under Title VI of the IAA for FY2014 (P.L. 113-126). That legislation, however, included no provisions for contractors.

Section 110 provides protections for IC contractors making a lawful complaint against any retaliatory personnel action involving an appointment, promotion/demotion, disciplinary or corrective action, detail, transfer or reassignment, suspension, termination, reinstatement, performance evaluation, decisions concerning pay, benefits, awards, education, or training. The protections extend to lawful complaints involving

a violation of any Federal law, rule or regulation (including with respect to evidence of another employee or contractor employee accessing or sharing classified information

⁵² 10 U.S.C. §1034(c)(4)(E).

⁵³ 10 U.S.C. §1034(e)(3)(A).

⁵⁴ 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.

⁵⁵ PPD-19 and ICD-120 do not address protections for contractors.

⁵⁶ P.L. 115-118, §110.

without authorization); or gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety.⁵⁷

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.⁵⁸

Section 110 also amended Section 3341(j) of Title 50, U.S. Code, to include protections for IC contractors who make lawful whistleblower disclosures against retaliatory revocation of their security clearances.

Resources to Enhance Whistleblower Investigations

House Amendment 894 to the DOD Appropriations Act for Fiscal Year 2015 (H.R. 4870), which was agreed to by a voice vote on June 18, 2014 but was not enacted, would have redirected \$2 million dollars to establish the IC Whistleblower and Source Protection Directorate. The funds, to augment the Intelligence Community Management Account, were to support the hiring of investigators and support staff to provide the ICIG greater ability to investigate fraud, waste, and abuse. Although it did not provide intrinsic protections for whistleblowers, the measure was intended to address an underfunded capability in order to enable responsive follow-up on whistleblower complaints.⁵⁹

Issues Raised by the IC Whistleblower Complaint of August 2019

The August 2019 whistleblower 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 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.⁶⁰

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.⁶¹ The ICIG supported his determination in a statement in which he indicated that the President's phone call

⁵⁷ 50 U.S.C. §3234(c)(1)(A)-(B). Unlike IC agency employees who are protected from reprisal for disclosures of "mismanagement," contractor employees are protected for disclosures of "gross mismanagement." See 50 U.S.C. §3234(b).

⁵⁸ See P.L. 115-118, §110(b)(1)-(5).

⁵⁹ See Department of Defense Appropriations Act for Fiscal Year 2015 (H.R. 4870, 113th Cong.), Title VII, Amendment Offered by Mr. Holt, pp. H5466-H5467, at <https://www.congress.gov/congressional-record/2014/06/18/house-section/article/H5454-2>.

⁶⁰ 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/>.

⁶¹ *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).

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.”⁶² 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.”⁶³
- 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.”⁶⁴

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.⁶⁵ According to the acting DNI’s congressional 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.⁶⁶

On September 3, 2019, the OLC, responding to a request by the General Counsel of the IC, issued an opinion on the complaint.⁶⁷ 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.”⁶⁸ The OLC suggested that, since the alleged wrongdoing did not

⁶² 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>.

⁶³ *Ibid.*, p. 4.

⁶⁴ *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>.

⁶⁵ 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.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>.

⁶⁶ *Ibid.*

⁶⁷ 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>.

⁶⁸ *Ibid.* The opinion cited the definition of “urgent concern” in 50 U.S.C. §3033(k)(5)(G)(i).

involve an intelligence activity, it fell outside the responsibility of the ICIG to investigate the complaint's credibility.⁶⁹

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.”⁷⁰ 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”).⁷¹

In a September 6, 2019, letter to the Chair and Ranking Member of the House Permanent Select Committee on Intelligence, the 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. The acting DNI's decision enabled the complainant to contact the committees directly “in an authorized and protected manner.”⁷²

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.⁷³

⁶⁹ Ibid., p. 10.

⁷⁰ Ibid., p. 5.

⁷¹ 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.

⁷² 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)

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 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>.

⁷³ *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>.

Proposed IC Whistleblower Legislation, 116th Congress

The political context surrounding the whistleblowing incident that led to the first impeachment of Donald J. Trump has raised discussion on whistleblowing generally. A 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 violation of law involving an intelligence activity. A retrospective analysis of IC whistleblowing legislation, whether passed or not, generally shows congressional encouragement for potential whistleblowers to report on issues that otherwise have limited means of oversight because of their classified nature. The circumstances of the 2019 whistleblowing incident exposed a number of areas with the potential to stimulate discussion on whether existing legislation meets Congress's original intent. These include (1) whether whistleblowers should have a right to remain anonymous, and, if so, what, if any, recourse do they have in the event their identity is disclosed against their will; (2) whether procedures provide potential whistleblowers clear direction on how to approach Congress with a protected disclosure; and (3) the final authority for making determinations of what constitutes a matter of "urgent concern." A number of these issues were raised in the 116th Congress. Bills introduced in the Senate and House would have amended the whistleblower provisions of the National Security Act of 1947; these provisions were not considered by either chamber. Provided here are summaries of the provisions included in Senate and House intelligence authorization bills that were not included in the enacted IAA for FY2021 but illustrate approaches to protecting whistleblowers.⁷⁴ Although the two bills generally addressed similar areas, an important difference is that the Senate version was specific to the ICIG while the House version applied to any inspector general of an IC element.

S. 3905, Intelligence Authorization Act (IAA) for Fiscal Year 2021 (Introduced)

Protection of a whistleblower's identity from disclosure

The bill would have added to existing whistleblower provisions more stringent prohibitions against "a knowing and willful or negligent disclosure revealing the identity or personally identifiable information" of a whistleblower.⁷⁵ The bill also would have prohibited sharing the identity of a whistleblower with the subject of a complaint without the whistleblower's written consent.⁷⁶ A whistleblower whose identity was disclosed in an unlawful, willful manner would be able to maintain a private right of action for redress.⁷⁷

Greater latitude for a whistleblower to report directly to Congress

Concern over a whistleblower's access to Congress was the subject of another provision that would have enabled a whistleblower to report a complaint—whether or not it had been

⁷⁴ For the enacted IAA for FY2021, see Division W of P.L. 116-260, the Consolidated Appropriations Act of 2021.

⁷⁵ S. 3905, §321(a)(3), at <https://www.congress.gov/bill/116th-congress/senate-bill/3905/text?r=3#toc-id3413DEA9BFD3469D8CC4A6B53BC394EB>.

⁷⁶ *Ibid.*, §324.

⁷⁷ *Ibid.*, §321(d)(2).

determined to be credible or a matter of urgent concern by the inspector general—directly to the leadership of the congressional intelligence committees or designated nonpartisan staff.⁷⁸

Expanded definition of “urgent concern”

The bill would have explicitly broadened the definition of “urgent concern” to include any serious or flagrant problem, abuse, violation of law or executive order, or deficiency not just concerning intelligence activities within the IC, but also activities “relating to the funding, administration, or operation of the Federal Government” and are “a matter of national security and not a difference of opinion concerning public policy matters.”⁷⁹

Independence of the ICIG

A provision also would have given the ICIG sole authority to determine whether a complaint constituted a matter of urgent concern.⁸⁰

H.R. 7856, Intelligence Authorization Act for Fiscal Year 2021 (Introduced)

Protection of a whistleblower’s identity from disclosure

H.R. 7856 would have provided additional protections against the unauthorized disclosure of a whistleblower’s identity. This would include the unauthorized disclosure of information in a complaint to an individual named in the complaint without the whistleblower’s written consent. An exception would be if the inspector general concerned or an attorney for the government determines—and gives prior notice to the whistleblower—that disclosure of the information is unavoidable to advance an investigation, audit, inspection, or evaluation.⁸¹

H.R. 7856 would have protected a whistleblower’s identity from disclosure as a reprisal for making a complaint.⁸² This section would have permitted a whistleblower to maintain a private right of action for “unlawful, willful disclosure” of the whistleblower’s identity.⁸³

Greater latitude for a whistleblower to report directly to Congress

The proposed House legislation was also similar to that in the Senate in expanding the means by which a whistleblower could report directly to the congressional intelligence committees. If the whistleblower were to choose to approach Congress directly to make a disclosure, the DNI or head of the IC element concerned, through the appropriate IC element inspector general, would have had to provide direction on how to safeguard classified information in doing so.⁸⁴

⁷⁸ Ibid., §323.

⁷⁹ Ibid., §322.

⁸⁰ Ibid.

⁸¹ H.R. 7856, Title V, §504(a).

⁸² Ibid., §506(a).

⁸³ Ibid., §506(c).

⁸⁴ Ibid., §505(a).

Expansion of the definition of “urgent concern”

H.R. 7856 would have expanded the definition of “urgent concern,” to include “a serious or flagrant problem, abuse, violation of law or Executive order, or deficiency relating to foreign interference in elections in the United States.”⁸⁵

Independence of IC Element Inspectors General

H.R. 7856 included protections for the independence of IC element inspectors general, including the ICIG. Principally, the proposed legislation would have limited the President’s ability to remove an inspector general of an element of the IC to instances of permanent incapacity, inefficiency, neglect of duty, malfeasance, felony conviction or “low moral turpitude,” substantial violations of laws, rules or regulations, gross mismanagement, gross waste of funds, and abuse of authority.⁸⁶

The bill also included limitations on the President’s ability to appoint an acting inspector general of an IC element to presidentially appointed, Senate-confirmed inspectors general positions of other organizations in the U.S. government, or the most senior career individual of the office of the inspector general in question holding a position in a senior executive service.⁸⁷

H.R. 7856 would have also given IC element Inspectors General “sole authority to determine whether any complaint or information reported to the Inspector General is a matter of urgent concern.”⁸⁸ That determination would have been final and conclusive.

Expansion of the responsibilities of the DNI

The bill would also have expanded the authority of the DNI to include “coordinating and supervising activities undertaken by elements of the intelligence community for the purpose of protecting the United States from any foreign interference in elections in the United States.”⁸⁹

Potential Questions for Congress

- What protections against disclosure of an IC whistleblower’s identity should exist in statute?
- What oversight, if any, should the DNI or the head of any IC intelligence element have in an ICIG or IC element inspector general’s determinations of the credibility of a complaint and what constitutes an urgent concern?
- Should the DNI be obligated to provide guidance on the protection of classified information in the event an IC whistleblower indicates an intention to report a complaint to Congress?
- What constitutes the scope of personal conduct that is reportable in an IC whistleblower complaint? What should be the scope of government activity that falls within a definition of urgent concern? What constitutes an intelligence activity?

⁸⁵ Ibid.

⁸⁶ H.R. 7856, §501(a).

⁸⁷ Ibid., §502(a).

⁸⁸ Ibid., §503(a)(1).

⁸⁹ Ibid.

- What is the extent to which the conduct of government officials outside the IC should be the subjects of an IC whistleblowing complaint?

Author Information

Michael E. DeVine
Analyst in Intelligence and National Security

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.