August 28, 2025

Administrative Investigations Manual

Office of the Deputy Inspector General for
Administrative Investigations

Contents

CHAPTER 1—INTRODUCTION

1.1 Purpose

1.1.1 This policies and procedures manual provides guidance to members of the DoD Office of Inspector General (DoD OIG), Office of the Deputy Inspector General for Administrative Investigations (ODIG AI), who conduct or perform oversight of administrative investigations into allegations of misconduct by senior DoD officials or whistleblower reprisal, and who operate the DoD Hotline. The guidance ensures that investigators and administrative investigations adhere to the "Quality Standards for Investigations" established in November 2011 by the Council of the Inspectors General on Integrity and Efficiency (CIGIE). The standards are summarized in Section 1.5 of this chapter and are incorporated where they apply in chapters throughout the manual.

1.1.2 This manual is only guidance. It does not create any right or benefit enforceable by law by any person against the United States or its agencies, officers, or employees. This manual does not create any right, entitlement, or privilege on the part of any person with respect to any official activity of the ODIG AI.

1.1.3 This manual is a living document. It will be updated periodically as policies and procedures are refined or changed in response to changes in law, rules, regulations, case law, and best practices.

1.2 Authority

1.2.1 Inspector General Act of 1978, as amended. The DoD Inspector General (IG) draws authority from the Inspector General Act of 1978, as amended (IG Act). Principal authorities under the Act that relate to the ODIG AI include:

1.2.1.1 Section 4(a)(1), to provide policy direction for and to conduct, supervise, and coordinate audits and investigations relating to the programs and operations of such establishment;

1.2.1.2 Section 6(a)(1), to have access to all records, reports, audits, reviews, documents, papers, recommendations, or other material available to the applicable establishment that relate to the programs and operations for which the Inspector General has responsibility under this Act;

1.2.1.3 Section 6(a)(5), to administer to or take from any person an oath, affirmation, or affidavit, whenever necessary in the performance of the functions assigned by this Act;

1.2.1.4 Section 7(a), to receive and investigate complaints or information concerning an activity constituting a violation of law, rule, or regulation, or mismanagement, gross waste of funds, abuse of authority, or a substantial and specific danger to the public health and safety;

1.2.1.5 Section 7(b), the IG will 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 IG determines such disclosure is unavoidable during the course of the investigation; and

1.2.1.6 Section 7(c), any employee who has authority to take, direct others to take, recommend, or approve any personnel action, shall not, with respect to such authority, take or threaten to take any action against any employee as a reprisal for making a complaint or disclosing information to an Inspector General.

1.2.2 DoD Directive (DoDD) 5106.01. The authorities vested in the DoD IG, under the IG Act are further implemented in the DoD under DoDD 5106.01, "Inspector General of the Department of Defense," April 20, 2012 (Incorporating Change 2, May 29, 2020).

1.3 ODIG AI Vision, Mission, and Authorities

The ODIG AI vision. Provide First-Class Service in Administrative Investigations and Hotline Operations

The ODIG AI mission. AI helps ensure ethical conduct throughout the DoD by conducting investigations and overseeing DoD Component investigations of allegations of misconduct by senior DoD officials, whistleblower reprisal, and Service member restriction from communication with an IG or Member of Congress. AI also manages the DoD Hotline and the Contractor Disclosure Program, provides education and training on whistleblower protections through its Whistleblower Protection Coordinator, and facilitates voluntary resolution of whistleblower reprisal allegations through its Alternative Dispute Resolution Program.

1.3.1 Investigations of Senior Officials. The ODIG AI Directorate for Investigations of Senior Officials (ISO) draws its authority from the IG Act, as well as authorities and responsibilities set forth in DoDD 5505.06, "Investigations of Allegations Against Senior DoD Officials," June 6, 2013 (Incorporating Change 1, April 28, 2020).

1.3.1.1 DoDD 5505.06. Under DoDD 5505.06, ISO is charged with responsibilities including: (1) receiving allegations against senior DoD officials; (2) notifying the DoD Components whether the DoD OIG will open an investigation or will refer the allegation to the DoD Component for investigation; and (3) providing oversight on investigations conducted by the other DoD Components.

1.3.1.2 DoD Instruction (DoDI) 1320.04. ISO is also responsible for performing checks of its investigative files under DoDI 1320.04, "Military Officer Actions Requiring Presidential, Secretary of Defense, or Under Secretary of Defense for Personnel and Readiness Approval or Senate Confirmation," January 3, 2014 (Incorporating Change 1, June 30, 2020). Under DoDI 1320.04, ISO checks its investigative files for adverse information relating to those military officers who have been nominated for personnel actions requiring the approval of the Secretary of Defense or the President, or confirmation by the Senate.

1.3.2 Whistleblower Reprisal Investigations. The ODIG AI Directorate for Whistleblower Reprisal Investigations (WRI) draws its authority from the IG Act, authorities and responsibilities under title 10 of the United States Code and their corresponding implementing regulations, and Presidential Policy Directive 19 (PPD-19) and its implementing regulations. The DoD OIG is

required by Federal statutes and Directives to review, investigate, and perform oversight of investigations of whistleblower reprisal cases as follows.

Section 1034, title 10, United States Code (10 U.S.C. § 1034). "Protected communications; prohibition of retaliatory personnel actions," prohibits taking, threatening to take, withholding, or threatening to withhold personnel actions against Service members in reprisal for making or preparing any protected communication. The statute also protects testifying or participating in or assisting in an investigation or proceeding related to a protected communication, and filing, causing to be filed, participating in, or otherwise assisting in an action under 10 U.S.C. § 1034.

Absent extraordinary circumstances, Service members are expected to file complaints of reprisal within 1 year of the personnel action occurring. The statute also prohibits restricting members of the armed forces from lawfully communicating with a Member of Congress or an Inspector General; complaints of restriction have no timeliness requirement for filing. DoDD 7050.06, "Military Whistleblower Protection," April 17, 2015 (Incorporating Change 1, October 12, 2021), updates established policies and assigned responsibilities, and otherwise implements the statute. (10 U.S.C. § 1034 and DoDD 7050.06)

1.3.2.1 For more information about investigating 10 U.S.C. § 1034 complaints, see DoDI 7050.09, "Uniform Standards for Evaluating and Investigating Military Reprisal or Restriction Complaints," October 12, 2021, and the DoD IG "Guide to Investigating Military Whistleblower Reprisal and Restriction Complaints," April 18, 2017. Section 1587, title 10, United States Code (10 U.S.C. § 1587), "Employees of nonappropriated fund instrumentalities: reprisals," prohibits taking or threatening to take or fail to take personnel actions against employees of nonappropriated fund instrumentalities in reprisal for making certain protected disclosures. Disclosures protected under 10 U.S.C. § 1587 include information reasonably believed to evidence a violation of any law, rule, or regulation; and mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety.

Disclosures involving information specifically required by or pursuant to executive order to be kept secret in the interest of national defense or the conduct of foreign affairs must be made to any civilian employee or member of the armed forces designated by law or by the Secretary of Defense to receive such disclosures. DoDD 1401.03, "DoD Nonappropriated Fund Instrumentality (NAFI) Employee Whistleblower Protection," June 13, 2014 (Incorporating Change 2, May 7, 2021), implements the statute (10 U.S.C. § 1587 and DoDD 1401.03).

1.3.2.2 Section 4701, title 10, United States Code (10 U.S.C. § 4701), "Contractor employees: protection from reprisal for disclosure of certain information," prohibits discharge, demotion, or other discrimination against DoD contractor or subcontractor employees in reprisal for making certain protected disclosures. Absent extraordinary circumstances, defense contractor or subcontractor employees are expected to file complaints of reprisal within 3 years of the alleged retaliatory action occurring. Intelligence Community Element contractors or subcontractors are not covered by 10 U.S.C. § 4701. Defense Federal Acquisition Regulation Supplement (DFARS) Subpart 203.9, "Whistleblower Protections For Contractor Employees" (added February 28, 2014), implements the statute (10 U.S.C. § 4701 and amendment, and DFARS Subpart 203.9). PPD-19 Part A, which applies to DoD employees in Defense Civilian Intelligence Personnel System (DCIPS) positions, prohibits various actions, including traditional personnel actions as well as decisions to order psychiatric testing or examination, in reprisal for making certain protected disclosures. PPD-19 Part B, which applies to DoD employees (including civilian employees, Service members, and contractor and subcontractor employees), prohibits taking, directing others to take,

recommending, or approving any action affecting an employee's eligibility for access to classified information, in reprisal for making certain protected disclosures.

Directive-Type Memorandum (DTM) 13-008, "DoD Implementation of Presidential Policy Directive 19," February 9, 2016, implements PPD-19 within the DoD.

1.3.2.3. Section 2302, title 5, United States Code (5 U.S.C. § 2302), "Prohibited personnel practices," and the IG Act. The U.S. Office of Special Counsel has primary jurisdiction to investigate complaints of reprisal filed by civilian appropriated fund employees throughout the Executive branch, including most DoD civilian appropriated fund employees. However, in matters of particular interest to the DoD IG, under the authority of Sections 7(a) and 8(c)(2) of the IG Act and DoDD 5106.01, the DoD IG may investigate, on a discretionary basis, complaints of reprisal from civilian appropriated-fund employees using as general guidance concepts consistent with 5 U.S.C. § 2302.

1.3.3. DoD Hotline. The ODIG AI Directorate for the DoD Hotline draws its authority from the IG Act, as well as authorities and responsibilities set forth in DoDI 7050.01, "Defense Hotline Program," December 17, 2007.

1.3.3.1. DoDI 7050.01 authorizes the DoD Hotline to task DoD Components and internal DoD OIG Components with resolving Hotline complaints through investigation, audit, or other means, and providing the Hotline with the results in a Hotline Completion Report.

1.4 Organization

1.4.1 DoD OIG. The DoD OIG was established under the IG Act to conduct, supervise, and coordinate audits and investigations relating to the programs and operations of the DoD.

The DoD OIG organizational structure includes the Inspector General, the Principal Deputy Inspector General, the Chief of Staff, and the Deputy Inspectors General for Administrative Investigations, Audit, Defense Criminal Investigative Service, Evaluations, and Overseas Contingency Operations. Some of the offices that provide support include the Office of Legislative Affairs and Communications; the Mission Support Team's offices of Strategic Planning and Performance; Human Capital Management; the Chief Information Officer; Security; Financial Management; and Communications; as well as other supporting functions.

The DoD OIG has a global presence with 89 offices located around the world.

1.4.2 ODIG AI. The ODIG AI comprises the ISO, WRI, DoD Hotline, and Front Office staff. The DoD Whistleblower Protection Coordinator (WPC) is aligned under the ODIG AI Front Office and is responsible for educating the DoD workforce on whistleblower protections.

1.4.3 ISO. The ISO Directorate conducts investigations into allegations against senior officials of the DoD and performs oversight of senior official investigations conducted by the Military Departments and Defense agencies. Senior officials are active duty, retired, Reserve, or National Guard military officers in grade O-7 and above, or selected to O-7; current and former members of the Senior Executive Service; and current or former Presidential appointees. ISO also performs checks of investigative records on the names of individuals who are pending military actions requiring approval by the Secretary of Defense or the President, or confirmation by the Senate.

1.4.4 WRI. The WRI Directorate objectively and thoroughly conducts, or provides oversight of Military Department and Component IG, investigations into allegations of whistleblower reprisal or restriction under the authorities pertaining to:

- members of the Military Service (Service members);
- appropriated and nonappropriated fund employees of the DoD;
- employees within the DoD Intelligence Community; and
- DoD contractor, subcontractor, grantee, sub-grantee, and personal services contractor employees.

The WRI Directorate operates an Alternative Dispute Resolution program, in which parties in certain cases may explore voluntary resolution of disputes in lieu of investigation.

1.4.5 DoD Hotline. The DoD Hotline Directorate operates the DoD Hotline program, directing its implementation in the DoD Components and ensuring that inquiries resulting from allegations are conducted in accordance with CIGIE standards and applicable laws, regulations, and policies. The DoD Hotline receives and investigates complaints or information concerning alleged violations of laws, rules, or regulations; mismanagement, gross waste of funds or abuse of authority; or a substantial and specific danger to public health and safety involving the DoD. The Contractor Disclosure Program is aligned within the DoD Hotline to facilitate self-reporting by DoD contractors to the OIG regarding fraud and other matters as mandated by the Close the Contractor Fraud Loophole Act of 2008.

1.5 The Council of the Inspectors General on Integrity and Efficiency

1.5.1 Quality Standards. The IG Act provides that members of CIGIE "shall adhere to professional standards developed by the Council." The CIGIE "Quality Standards for Investigations," November 2011, sets forth the professional standards and principles for investigators of the Federal Offices of Inspectors General. The standards apply to OIG criminal and administrative investigations.

1.5.2 General Standards

1.5.2.1 Qualifications. Individuals assigned to conduct the investigative activities of the ODIG AI must possess professional proficiency for the tasks required.

1.5.2.2 Character. Each investigator must possess and maintain the highest standards of conduct and ethics, including unimpeachable honesty and integrity.

1.5.2.3 Independence. In all matters relating to investigative work, the investigative organization must be free, both in fact and appearance, from impairments to independence; must be organizationally independent; and must maintain an independent attitude.

1.5.2.3.1 Personal. Personal impairments can include personal or financial relationships, preconceived biases, or prior involvement in the entity or program being investigated.

1.5.2.3.2 External. External impairments can include interference in the exercise of investigative responsibility, restriction on funds or resources, authority to overrule or influence the investigation, or the denial of access to records or sources of information.

1.5.2.3.3 Organization. The investigative organization must be organizationally located outside the staff or the line management of the unit under investigation.

1.5.2.4 Due Professional Care. Investigators should use due professional care in conducting investigations and in preparing related reports.

1.5.2.4.1 Thoroughness. All investigations must be conducted in a diligent and complete manner, and reasonable steps should be taken to ensure pertinent issues are sufficiently resolved.

1.5.2.4.2 Legal. Investigations should be conducted in accordance with all applicable laws, rules, and regulations, and with due respect for the rights and privacy of those involved.

1.5.2.4.3 Impartiality. All investigations must be conducted in a fair and equitable manner, with the perseverance necessary to determine the facts.

1.5.2.4.4 Objectivity. Evidence must be gathered and reported in an unbiased and independent manner in an effort to determine the validity of an allegation or to resolve an issue.

1.5.2.4.5 Ethics. At all times, the actions of the investigator and the investigative organization must conform to generally accepted standards of conduct for Government employees.

1.5.2.4.6 Timeliness. All investigations must be conducted and reported with due diligence and in a timely manner. This is especially critical given the impact investigations have on the lives of individuals and the activities of organizations.

1.5.2.4.7 Documentation. The investigative report findings and investigative accomplishments must be supported by adequate documentation.

1.5.2.4.8 Policies and Procedures. To facilitate due professional care, organizations should establish written investigative policies and procedures.

1.5.3 Qualitative Standards

1.5.3.1 Planning. Organizational and case-specific priorities must be established and objectives developed to ensure that individual case tasks are performed efficiently and effectively.

1.5.3.2 Execution. Investigations must be conducted in a timely, efficient, thorough, and legal manner. The investigator is a fact-gatherer and should not allow conjecture,

unsubstantiated opinion, or bias to affect this work. The investigator also has a duty to be receptive to evidence that is non-incriminating as well as incriminating.

1.5.3.3 Reporting. Reports must thoroughly address all relevant aspects of the investigation and be accurate, clear, complete, concise, logically organized, timely, and objective.

1.5.3.4 Information Management. Investigative data must be stored in a way that allows effective retrieval, referencing, and analysis.

1.6 Recusals

During the intake process or at any point during the handling of a complaint, including investigation, assigned personnel who may have a real or perceived conflict of interest in the outcome of the case must consult with their supervisors. If a decision is made that a person should be recused, that person must write a memorandum explaining the reason for recusal, submit it to an Office of General Counsel (OGC) ethics advisor for review, and then provide it to the supervisor. The recusing person will then document the recusal in the appropriate field in Defense-Case Activity Tracking System Enterprise (D-CATSe), and the supervisor will reassign the case. Staff must provide a copy of the recusal memorandum to the Principal Assistant Inspector General and the AI Program Analyst (Quality Assurance).

CHAPTER 2—COMPLAINT INTAKE

2.1 Sources of Complaints

2.1.1 D-CATSe. Cases are received from the DoD Component IGs and the DoD Hotline via D-CATSe, the system of record for case files and case-related information. The entire life cycle of a complaint is documented in D-CATSe.

2.1.2 DoD Hotline. The DoD Hotline is a DoD-level program office that provides Service members, DoD civilian employees and contractor employees, and members of the public a confidential channel for reporting fraud, waste, abuse, allegations of reprisal, and other misconduct. The DoD Hotline staff receives complaints via telephone, the DoD Hotline public website, and other means of communication.

2.1.3 DoD Hotline Referrals. The DoD Hotline is one of the primary sources of complaints received by ISO and WRI. On receipt of complaints, DoD Hotline staff perform an initial screening and refer those involving allegations of whistleblower reprisal or misconduct by senior officials to WRI or ISO via the electronic case management system (D-CATSe).

2.1.4 Military Departments and DoD Component IG Notifications. The other primary source of complaints received by the ODIG AI is the notification of allegations of whistleblower reprisal or senior official misconduct from the Military Departments and DoD Components through their OIGs, Internal Review, or other channels. Notifications are required by DoDD 7050.06 and DoDD 5505.06.

2.1.5 Third-Party Complaints of Reprisal. If a party alleges that someone else has been reprised against, WRI will contact the aggrieved party, if possible, to determine if the aggrieved party wishes to file a complaint.

2.1.6 Required Notifications. Under DoDD 7050.06, which covers military reprisal and restriction complaints, the Military Departments are required to notify the DoD OIG within 10 days after receiving a reprisal or restriction allegation involving sexual assault, matters of known congressional interest, or senior officials. For all other reprisal or restriction allegations, notification is due within 30 days after receipt. Furthermore, the DoD Intelligence Component IGs are required to notify the DoD OIG of any nonfrivolous allegations involving Service members that they receive directly, generally within 10 working days, unless otherwise agreed to by the DoD OIG and the respective DoD Intelligence Component IG. Under DTM 13-008 DoD Component IGs are required to notify the DoD OIG within 10 workdays of receiving any allegations of reprisal covered by PPD-19. Under DoDD 5505.06, the DoD Component heads are required to notify the DoD OIG of all allegations of misconduct made against senior officials within 5 workdays of receipt.

2.1.7 Congressional Inquiries. Another source of complaints received by the ODIG AI are those forwarded by Members of Congress on behalf of a constituent or requests for investigation from Members or congressional committees. These complaints will be initially received and processed by the Office of Legislative Affairs and Communication (OLAC). Upon receipt, an OLAC staff member prepares the initial acknowledgement letter to the interested Member and refers the congressional inquiries to the appropriate DoD OIG Components.

2.2 Case Intake—ISO

2.2.1 ISO Definitions:

- Intake: Intake refers broadly to the receipt of the complaint, initial review, and, if appropriate, initial investigative work to determine whether the case warrants investigation.

- Investigation: Investigation refers to those cases that ISO has reviewed in the intake process, determined that the allegations warrant investigation as a matter of senior official misconduct, and referred for investigation.

2.2.2 ISO Intake Process. The ISO intake process consists of a review of the incoming complaint, and as appropriate, investigative work (also referred to as "complaint clarification") to determine whether the complaint contains allegations of misconduct that warrant further investigation. Investigative work conducted during the intake process may include an interview with the complainant or potential witnesses. Complaint clarification may also include requesting documents, such as, but not limited to, travel vouchers or time and attendance records.

After an evaluation of the allegations and any facts or evidence gathered during the intake process, the DoD OIG will make one of the following determinations.

- Close the case.

- Retain the case in ISO.

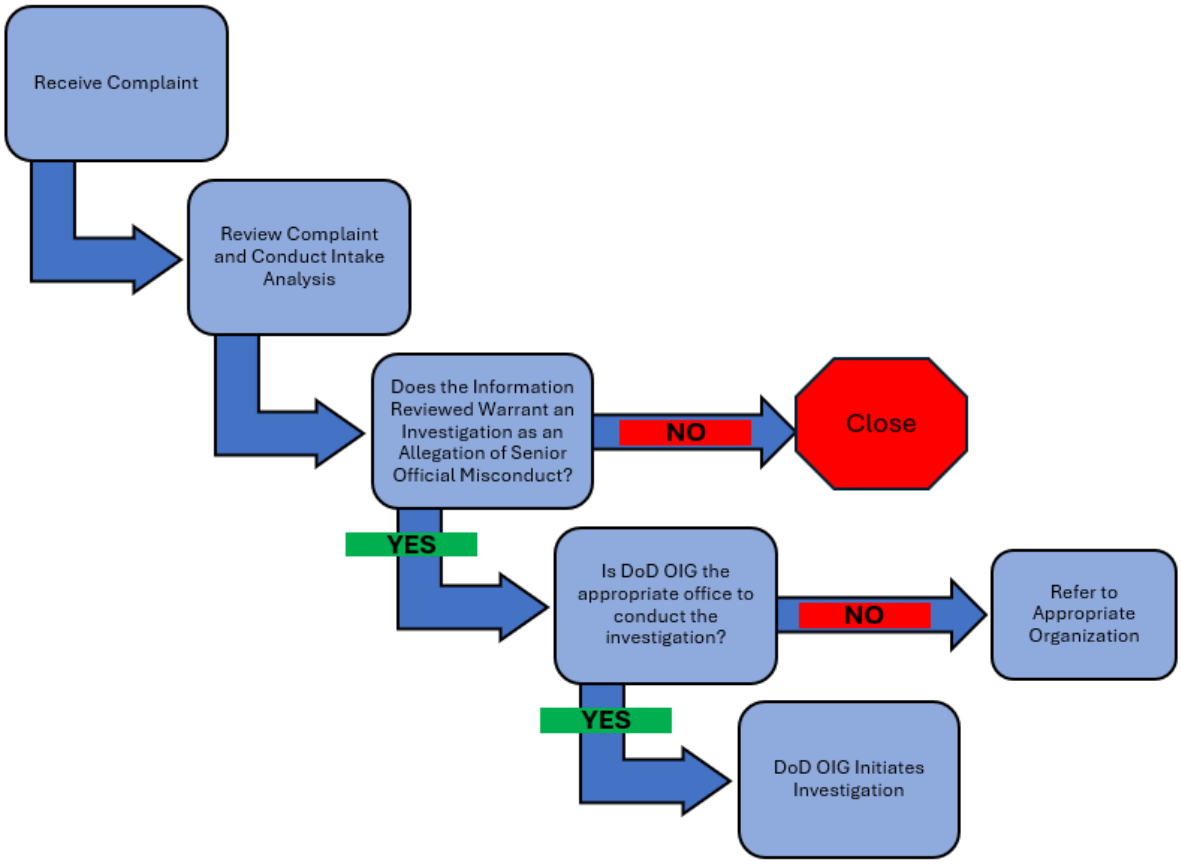
- Refer the case to a DoD Component IG, or other appropriate organization, for further complaint clarification or investigation.

A decision to close a case does not preclude other appropriate action such as a referral to another organization for review or action.

In general, the DoD OIG may close a case during the intake process in the following situations.

- The allegations do not include an allegation of misconduct.
- The allegations do not include sufficient information with which to conduct a focused review.
- The allegations, if true, would not constitute a violation of law, rule, or other regulations.
- The allegations involve issues that are more appropriate to be addressed in other channels (for example, requests for relief to the Service Board for Correction of Military Records (BCMR), appeals of an evaluation report, appeals of adverse administrative actions, appeals of punishment under Article 15 of the Uniform Code of Military Justice (UCMJ), complaints submitted to an equal employment opportunity (EEO) office, complaints of administrative grievance, requests for assistance or redress to the chain of command).

Figure 2.1 ISO Intake Workflow



2.3 Case Intake—WRI

2.3.1 WRI Intake Definitions

- Inquiry. Refers to any type of investigative review to ascertain the facts in response to a DoD Hotline or Component hotline referral. The term used in D-CATSe is "Office of Inquiry," meaning the office responsible for handling a matter.Intake. The initial investigative stage in which we conduct the complaint evaluation and clarification process to determine whether a complaint contains *prima facie* allegations of whistleblower reprisal or restriction and whether the complaint, based on the facts readily available in Intake, warrants investigation.

- *Prima Facie*. Black's Law Dictionary defines a *prima facie* case as one that is established by sufficient evidence, and can be overthrown only by rebutting evidence introduced by the other side.

- Investigation. The investigative activity and steps to ensure that allegations are thoroughly and objectively resolved. Investigations include interviewing complainants, witnesses, and subjects; collecting documentary and other evidence; and documenting findings and conclusions in written reports that will be found legally sufficient.

2.3.2 Purpose of WRI Intake Process. The intake process will determine whether complaints alleging reprisal or restriction provide sufficient evidence to warrant an investigation—that is, whether the available evidence is sufficient to establish the elements of a *prima facie* allegation and currently, insufficient evidence exists to clearly and convincingly establish that the action was taken for reasons other than reprisal.[1] Figure 2.2 shows the WRI intake workflow.

- The Supervisory Investigator (SI) reviews the complaint and assigns it to an investigator.

- Review of the Entire Complaint. The investigator will verify the Complainant is covered by a statute administered by the DoD OIG and review the alleged restriction, or, if reprisal, the PDs or PCs to whom they were made, when they were made, and any alleged prohibited PAs.

- Acknowledgment of Complaint. As soon as practicable after case assignment, the investigator will contact the Complainant to advise that the complaint was received and schedule a clarification interview, if appropriate.

- Clarification Interview. The investigator will conduct a clarification interview to fully understand the allegations and document the PC/PDs, PAs, and other elements associated with the complaint.

- Additional Information. The investigator will also request that the Complainant provide any additional information or documentation in their possession related to the PC/PDs,

[1] We use a "clear and convincing" standard to determine whether to dismiss a reprisal allegation at the Intake stage, the evidentiary standard during the Investigation stage for 10 U.S.C. §§ 1034 and 1587 is a preponderance of the evidence.

PAs, or that would establish knowledge, motive, or would otherwise indicate a causal connection.

2.3.3 Does the complaint, as supplemented by the interview of the Complainant, establish a *prima facie* allegation by including the following?

- Protected Communication/Disclosure. Does the evidence establish that the Complainant made a PC or PD or was perceived as having made a PC or PD?

- Personnel Action. Does the evidence establish that the Complainant was the subject of a qualifying PA under the relevant statute/directive?

- Knowledge/Contributing Factor. Does timing or subject knowledge support the inference that the alleged PC/PD was a contributing factor in the action taken or not taken with respect to the Complainant?

If the three factors above are present, the evidence supports a *prima facie* allegation of reprisal.

However, in determining whether the complaint warrants investigation, the DoD OIG evaluates all evidence collected during the intake process to determine if the facts and evidence warrant initiating an investigation.

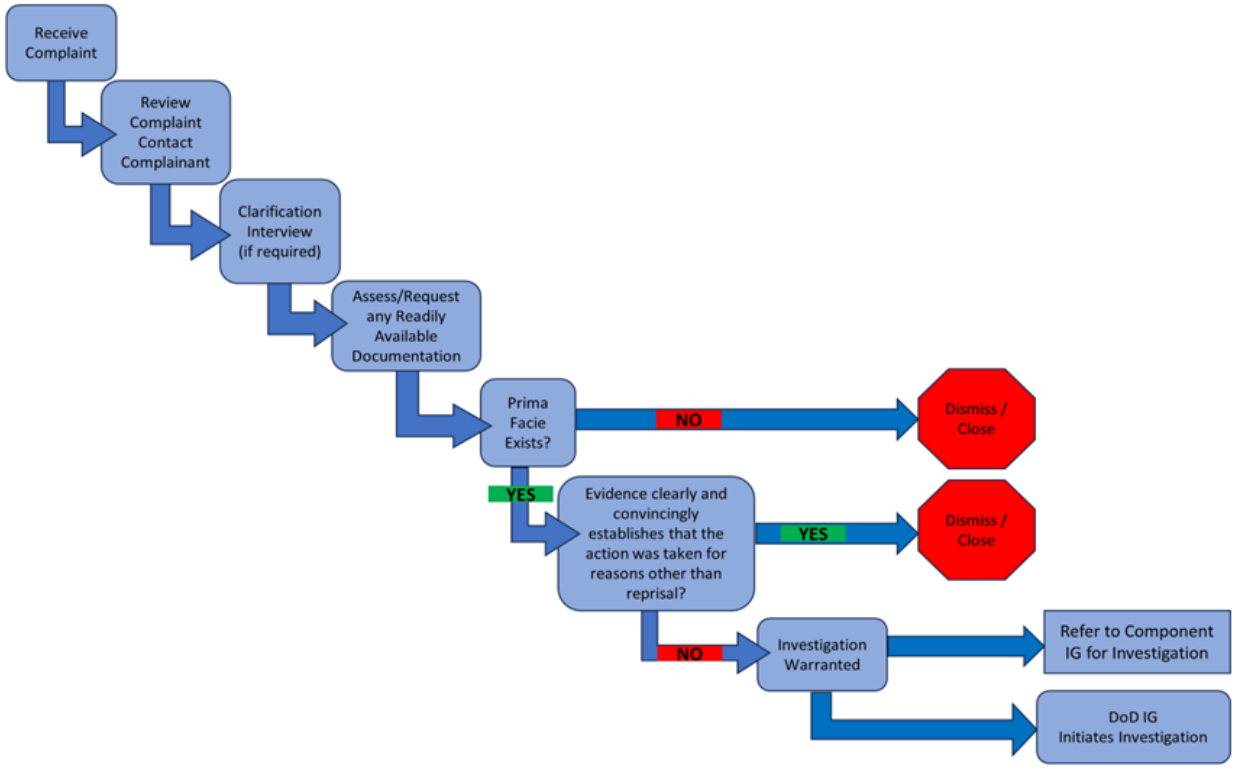
2.3.4 Causation. Do the facts support an inference of reprisal that warrants investigation? The DoD OIG will evaluate whether the facts/evidence collected in the Intake phase suggest that the PD could have been factor in an action. Items to consider when assessing whether the PD/PC could have been a contributing factor in the PA include the following.

- Motive: The PD/PC was about something that would give the subject motive to reprise, or the subject has expressed animosity concerning a PD/PC made by the Complainant.

- Disparate Treatment: Was the Complainant treated less favorably than similarly situated nonwhistleblowers?

- Strength of Available Evidence Supporting the Action: Does the available evidence collected during the Intake phase, and discussed with the Complainant, clearly and convincingly establish that the basis for the action was taken for reasons other than reprisal (was unrelated to the PD/PC)?

Figure 2.2 WRI Intake Workflow



2.4 WRI Authorities

2.4.1 10 U.S.C. § 1034 – Restriction.

2.4.1.1 Persons covered by the statute. Service members.

2.4.1.2 Timeliness. Allegations of restriction can be filed at any time; they are not subject to a time limit to file.

2.4.1.3 Restriction analysis. The investigator must analyze whether the subject said or did something that a reasonable person could believe that, if true, would have deterred a similarly situated Service member from lawfully communicating with a Member of Congress or an IG.

2.4.2 Title 10 U.S.C. § 1034 – Reprisal.

2.4.2.1 Persons covered by the statute. Current and former Service members.

2.4.2.2 Timeliness. If during the intake process it becomes apparent that the complaint was not filed within 1 year of the Complainant becoming aware of the most recent alleged PA, consider whether the untimely complaint filing should be accepted based on compelling

reasons or circumstances. These circumstances may include situations in which the Service member:

- was actively misled regarding their rights;
- was prevented in some extraordinary way from exercising their rights; or
- filed the same allegation within the 1-year period with the wrong office or agency.

If no compelling reasons or circumstances exist, the case may be dismissed as untimely.

2.4.2.3 Reprisal analysis. Does the complaint, as supplemented by the interview of the complainant, establish a *prima facie* allegation by including the following?

- Protected Communication. See Table 2.3.2.a. and DoDD 7050.06. Does the evidence establish that the Complainant made or was preparing to make a PC to a qualified recipient or that they were perceived as making or preparing to make a PC?
- Personnel Action. See Table 2.3.2.b. Does the evidence establish that an unfavorable PA was taken or threatened against the Complainant, or that a favorable PA was withheld or threatened to be withheld from them?
- Knowledge. Do the alleged facts support an inference that the subject knew of the PC or perceived the Complainant as making or preparing to make a PC, before the PA?
- Causation. Do the facts support an inference of reprisal that warrants investigation? The DoD OIG will evaluate whether all of the facts/evidence collected in the Intake phase suggest that the PC could have been a factor in the PA. Items to consider when assessing whether a causal connection exists between the PC(s) and PA(s) include the following.
    - Temporal Proximity. The PA followed closely behind the PC, or the timing and sequence of events indicates a PC could have been a factor in a PA.
    - Motive. The PC was about something that would give the subject motive to reprise, or the subject has expressed animosity concerning a PC made by the Complainant.
    - Disparate Treatment. Was the Complainant treated consistently with other similarly situated nonwhistleblowers?
    - Strength of Available Evidence Supporting the PA. Does the available evidence collected during the Intake phase clearly and convincingly establish that the basis for the action was unrelated to the PC (no causal connection)?

Table 2.3.2.a. 10 U.S.C. § 1034 Protected Communication

Type of Communication	Conditions on Protection	When Made To
Any communication	Must be a lawful communication	• a Member of Congress or • an IG
Any communication in which a Service member communicates information that he or she reasonably believes evidences: • a violation of law or regulation, including a law or regulation prohibiting rape, sexual assault, or other sexual misconduct in violation of sections 920, 920b, 920c, or 930 of this title (article 120, 120b, 120c, or 130 of the UCMJ),* sexual harassment, or unlawful discrimination; • gross mismanagement, a gross waste of funds or other resources, an abuse of authority, or a substantial and specific danger to public health or safety; • a threat by another Service member or employee of the U.S. Government that indicates a determination or intent to kill or cause serious bodily injury to Service members or civilians or damage to military, Federal, or civilian property; • testimony, or otherwise participating in or assisting in an investigation or proceeding related to a communication as described above; or • filing, causing to be filed, participating in, or otherwise assisting in a military whistleblower reprisal action.	A communication will not lose its protected status because: • the communication was made to a person who participated in the activity that the Service member complained of; • the communication revealed information that had been previously disclosed; • of the Service member's motive for making the communication; • the communication was not in writing; • the communication was made while the Service member was off duty; or • the communication was made during the normal course of the Service member's duties.	a Member of Congress; an IG; • a member of a DoD audit, inspection, investigation, or a law enforcement organization; • any person or organization in the chain of command; • a court-martial proceeding; or • any other person or organization designated pursuant to regulations or other established administrative procedures to receive such communications.

Source: DoDD 7050.06.

* DoDD 7050.06, as amended in 2021, incorrectly references Title 5, U.S.C., sections 920 through 920c. The correct reference is Title 10, U.S.C., section s 920, 920b, 920c, or 930 of this title (article 120, 120b, 120c, or 130 of the UCMJ).

Gross Mismanagement
DoDD 7050.06 defines "gross mismanagement" as a "management action or inaction that creates a substantial risk of significant adverse impact on the agency's ability to accomplish its mission. The matter must be significant and more than de minimis wrongdoing or simple

negligence. It does not include management decisions that are merely debatable among reasonable people."

Abuse of Authority
DoDD 7050.06 defines "abuse of authority" as an "arbitrary or capricious exercise of power by a military member or a federal official or employee that adversely affects the rights of any person or results in personal gain or advantage to himself or herself or to preferred other persons."

Gross Waste of Funds
DoDD 7050.06 defines "gross waste of funds" as an "expenditure that is significantly out of proportion to the benefit reasonably expected to accrue to the government."

Substantial and Specific Danger to Public Health or Safety
DoDD 7050.06 does not define "substantial and specific danger to public health or safety." Although not binding in Military Whistleblower Protection Act cases, case law developed under the Whistleblower Protection Act (WPA) for appropriated fund Federal civilian employees may be used as a general guide. This case law holds that "substantial and specific danger to public health or safety" is determined by (1) the likelihood of harm resulting from the danger, (2) when the alleged harm may occur, and (3) the nature of the harm—the potential consequences.

Table 2.3.2.b. 10 U.S.C. § 1034 Personnel Action

Personnel Action
DoDD 7050.06 defines a "personnel action" as any action taken on a Service member that affects, or has the potential to affect, that member's military pay, benefits, or career. Such actions include: • threatening to take any unfavorable action; • withholding, or threatening to withhold, any favorable action; • making, or threatening to make, a significant change in the duties or responsibilities of a Service member not commensurate with the member's grade; • 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; • conducting a retaliatory investigation of a Service member; and • referral for mental health evaluation in accordance with DoD Instruction 6490.04. Personnel actions may be either favorable or unfavorable. • Favorable personnel actions are those that are reasonably expected to result in a positive impact on the Service member's military pay, benefits, or career. They do not include inconsequential matters. • Unfavorable personnel actions are those that are reasonably expected to result in an adverse impact on the Service member's military pay, benefits, or career. They do not include inconsequential matters.

Source: DoDD 7050.06.

2.4.3 Title 10 U.S.C. § 1587

2.4.3.1 Persons covered by the statute. NAFI employees, former employees, and applicants.

2.4.3.2 Timeliness. Allegations of reprisal, under 10 U.S.C. § 1587, can be filed at any time; they are not subject to a time limit to file.

2.4.3.3 Reprisal analysis. Does the complaint, as supplemented by the interview of the Complainant, establish a *prima facie* allegation by including the following?

- Protected Disclosure. See Table 2.3.3.a. Does the evidence establish that the Complainant made or was preparing to make a PD or that they were perceived as having made a PD?

- Personnel Action. See Table 2.3.3.b. Does the evidence establish that a subject has taken or failed to take, or threatened to take or fail to take, a PA against the Complainant?

- Knowledge. Do the alleged facts support an inference that the subject knew of the PD or perceived the Complainant as making or preparing to make a PD before the PA?

- Causation. Do the alleged facts support an inference of reprisal that warrants investigation? The DoD OIG will evaluate whether all of the facts/evidence collected in the Intake phase suggest that the PD could have been a factor in the PA. Items to consider when assessing whether a causal connection exists between PD(s) and PA(s) include the following.

    - Temporal Proximity: The PA followed closely behind the PD, or the timing and sequence of events indicates a PD could have been a factor in a PA.

    - Motive: The PD was about something that would give the subject motive to reprise, or the subject has expressed animosity concerning a PD made by the Complainant.

    - Disparate Treatment: Was the Complainant treated consistently with other similarly situated nonwhistleblowers?

    - Strength of Available Evidence Supporting the PA: Does the available evidence collected during the intake phase clearly and convincingly establish that the basis for the action was unrelated to the PD (no causal connection)?

Table 2.4.3.a. 10 U.S.C. § 1587 Protected Disclosure

Protected Disclosure
A protected disclosure under 10 U.S.C. § 1587, as implemented by DoDD 1401.03, "DoD Nonappropriated Fund Instrumentality (NAFI) Employee Whistleblower Protection," June 13, 2014, (Incorporating Change 3, April 5, 2023), is a disclosure of information by an employee, former employee, or applicant that the employee, former employee, or applicant reasonably believes evidences: • a violation of any law, rule, or regulation; • mismanagement; • a gross waste of funds; • an abuse of authority; or • a substantial and specific danger to public health or safety. Section 1587, title 10, U.S.C., as implemented by DoDD 1401.03, does not require that such disclosures be made to any particular recipient unless the disclosure is specifically prohibited by law or the information is specifically required by or pursuant to executive order to be kept secret in the interest of national defense or the conduct of foreign affairs. Disclosures related to information prohibited by law from release, and in which the information is specifically required by, or pursuant to executive order to be kept secret in the interest of national defense or the conduct of foreign affairs, must be made to a civilian employee or Service member designated by law or the Secretary of Defense to receive such disclosures.

Mismanagement
DoDD 1401.03 defines "mismanagement" as "[w]rongful or arbitrary and capricious actions that may have an adverse effect on the efficient accomplishment of the agency's mission."

Abuse of Authority
DoDD 1401.03 defines "abuse of authority" as an "arbitrary and capricious exercise of power by a military member or a Federal official or employee that adversely affects the rights of any person or that results in personal gain or advantage to himself or herself or to preferred other persons."

Gross Waste of Funds
DoDD 1401.03 defines "gross waste of funds" as an "expenditure that is significantly out of proportion to the benefit expected to accrue to the government."

Substantial and Specific Danger to Public Health or Safety Mismanagement
Neither 10 U.S.C. § 1587 nor DoDD 1401.03 defines "substantial and specific danger to public health or safety." As guidance, case law developed under the WPA holds that "substantial and specific danger to public health or safety" is determined by (1) the likelihood of harm resulting from the danger, (2) when the alleged harm may occur, and (3) the nature of the harm—the potential consequences.

Table 2.4.3.b. 10 U.S.C. § 1587 Personnel Action

Personnel Action (NAFI)
DoDD 1401.03 defines a "personnel action" with respect to a NAFI employee, former employee, or applicant as: • an appointment; • a promotion; • a disciplinary or corrective action; • a detail, transfer, or reassignment; • a reinstatement, restoration, or reemployment; • a decision concerning pay, benefits, awards, or concerning education or training if the education or training may reasonably be expected to lead to an appointment, promotion, or other action described in this section; or • any other significant change in duties or responsibilities that is inconsistent with the employee's salary or grade level.

Source: DoDD 1401.03.

2.4.4 Title 10 U.S.C. § 4701

2.4.4.1 Persons covered by the statute. Employees of DoD contractors, subcontractors, grantees, subgrantees, and personal services contractors. Excludes contractors subcontractors, grantees, subgrantees, or personal services contractors of an element of the intelligence community as defined in 50 U.S.C. § 3003.

2.4.4.2 Timeliness. The Complainant must file within 3 years of the date on which the Complainant became aware of the company's decision to discharge, demote, or take or fail to take another action with respect to the Complainant.

2.4.4.3 Reprisal analysis. Does the complaint, as supplemented by the interview of the Complainant, establish a *prima facie* allegation by including the following?

- Protected Disclosure. See Table 2.3.4.a. Does the evidence establish that the Complainant made a PD or was perceived as having made a PD?

- Discharge, Demotion, or Otherwise Discriminated Against. Does the evidence establish that the subject discharged, demoted, or otherwise discriminated against the Complainant? In evaluating whether the Complainant was otherwise discriminated against, determine whether the subject took any other action with respect to the Complainant that might have dissuaded a reasonable employee from making a PD.

- Knowledge/Contributing Factor. See Table 2.3.4.b. Does timing or subject knowledge support the inference that the alleged PD was a contributing factor in the action taken or not taken with respect to the Complainant?

If these three factors above are present, the evidence supports a *prima facie* allegation of reprisal. However, the DoD OIG evaluates any additional evidence collected during the

intake process in making its decision to determine if the facts and evidence warrant initiating an investigation—specifically, the following.

- Causation. Do the facts support an inference of reprisal that warrants investigation? Evaluate whether all of the facts/evidence collected in the Intake phase suggest that the PD could have been a factor in an action. Items to consider when assessing whether a causal connection exists between the PD(s) and the action include the following.
    - Temporal Proximity: The action followed closely behind the PD, or the timing and sequence of events indicates a PD could have been a factor in an action.
    - Motive: The PD was about something that would give the subject motive to reprise, or the subject has expressed animosity concerning a PD made by the Complainant.
    - Disparate Treatment: Was the Complainant treated consistently with other similarly situated nonwhistleblowers?
    - Strength of Available Evidence Supporting the Action: Does the available evidence collected during the Intake phase clearly and convincingly establish that the basis for the action was unrelated to the PD (no causal connection)?

Table 2.4.4.a. 10 U.S.C. § 4701 Protected Disclosures

Types of Disclosure	When Made To
Information reasonably believed to evidence: • gross mismanagement of a DoD contract or grant; • a gross waste of DoD funds; • a substantial and specific danger to public health or safety; • a violation of law, rule, or regulation related to a DoD contract (including the competition for or negotiation of a contract) or grant; or • abuse of authority relating to a DoD contract or grant	• a Member of Congress • a representative of a committee of Congress; • an Inspector General; • the Government Accountability Office; • a DoD employee responsible for contract oversight or management; • the Department of Justice or an authorized official of a law enforcement agency; • a court, grand jury, or any judicial or administrative hearing (as clarified in the DFARS: "An employee who initiates or provides evidence of contractor or subcontractor misconduct in any judicial or administrative proceeding relating to waste, fraud, or abuse on a DoD contract shall be deemed to have made a disclosure."; or • a management official or other employee of the contractor or subcontractor who has the responsibility to investigate, discover, or address misconduct.
Providing evidence of contractor or subcontractor misconduct	When disclosed in the course of initiating or providing evidence to any judicial or administrative proceeding relating to waste, fraud, or abuse on a DoD contract

Source: The DoD OIG.

Gross Mismanagement
Case law developed under the WPA defines "gross mismanagement" as "a management action or inaction that creates a substantial risk of significant adverse impact on the agency's ability to accomplish its mission." The matter must be significant and more than minor wrongdoing or simple negligence. It does not include management decisions that are merely debatable among reasonable people.

Gross Waste of Funds
Case law developed under the WPA defines "gross waste of funds" as "an expenditure that is significantly out of proportion to the benefit reasonably expected to accrue to the government."

Substantial and Specific Danger to Public Health or Safety
Case law developed under the WPA holds that "substantial and specific danger to public health or safety" is determined by (1) the likelihood of harm resulting from the danger, (2) when the alleged harm may occur, and (3) the nature of the harm—the potential consequences.

Abuse of Authority
10 U.S.C. § 4701 defines "abuse of authority" as "an arbitrary and capricious exercise of authority that is inconsistent with the mission of the Department of Defense or the successful performance of a Department contract or grant."

Table 2.4.4.b. 10 U.S.C. § 4701 Contributing Factor

Contributing Factor
Any protected disclosure that affects the decision to take, threaten to take, withhold, threaten to withhold, or fail to take an action with respect to the individual who made the disclosure.

Source: The DoD OIG.

2.4.5 PPD-19 – Part A.

2.4.5.1 Persons covered by the directive. Defense Civilian Intelligence Personnel System (DCIPS) employees.

2.4.5.2 Timeliness. Allegations of reprisal, under PPD-19 Part A, can be filed at any time; they are not subject to a time limit to file.

2.4.5.3 Reprisal analysis. Does the evidence, as supplemented by the interview of the Complainant, establish a *prima facie* allegation by including the following?

- Protected Disclosure or Activity. See Table 2.3.5.a. Has the evidence established that the Complainant made a PD or was perceived as having made a PD; exercised any appeal, complaint, or grievance with regard to a violation of Part A or B of PPD-19; lawfully participated in an investigation or proceeding regarding a violation of Section A or B of PPD-19; cooperated with or disclosed information to an IG, in general accordance with applicable provisions of law in

connection with an audit, inspection, or investigation conducted by the IG; or reported a matter of urgent concern to Congress?

- Personnel Action. See Table 2.3.5.b. Does the evidence establish that the Complainant was the subject of a qualifying PA?

- Knowledge/Contributing Factor. Does timing or subject knowledge support that the alleged PD was a contributing factor in the actual or threatened PA?

If these three factors above are present, the evidence supports a *prima facie* allegation of reprisal. However, the DoD OIG also evaluates any additional evidence collected during the intake process in making its decision to determine if the facts and evidence warrant initiating an investigation, specifically the following.

- Causation. Do the facts support an inference of reprisal that warrants investigation? Evaluate whether all of the facts/evidence collected in the Intake phase suggest that the PD could have been a factor in a PA. Items to consider when assessing whether a causal connection exists between the PD(s) and the PA include the following.

  - Temporal Proximity. The PA followed closely behind the PD, or the timing and sequence of events indicates a PD could have been a factor in a PA.

  - Motive. The PD was about something that would give the subject motive to reprise, or the subject has expressed animosity concerning a PD made by the Complainant.

  - Disparate Treatment. Was the Complainant treated consistently with other similarly situated nonwhistleblowers?

  - Strength of Available Evidence Supporting the Action. Does the available evidence collected during the Intake phase clearly and convincingly establish that the basis for the PA was unrelated to the PD (no causal connection)?

Table 2.4.5.a. PPD-19 Protected Disclosure

Types of Disclosure	When Made To
1. Disclosure of information that the employee reasonably believes evidences: • a violation of any law, rule, or regulation, • gross mismanagement, • a gross waste of funds, • an abuse of authority, or • a substantial and specific danger to public health or safety. 2. Exercise of any appeal, complaint, or grievance with regard to the violation of Section A or B of PPD-19. [1]	1 – 4: • a supervisor in the employee's direct chain of command up to and including the head of the employing agency, • the IG of the employing agency or Intelligence Community Element, • the Director of National Intelligence, • the IG of the Intelligence Community, or • an employee designated by any of the above officials for the purpose of receiving such disclosures.

Types of Disclosure	When Made To
3. Lawfully participating in an investigation or proceeding regarding a violation of Section A or B of this directive. [2] 4. Cooperating with or disclosing information to an IG, in accordance with applicable provisions of law in connection with an audit, inspection, or investigation conducted by the IG.[3] 5. Reporting matters of urgent concern under subsections The IG Act at 5 U.S.C. § 416(b)(1), (e), & (a).	5. To Congress, via the DoD OIG.

Source: The DoD OIG.

[1] "… if the actions described under subparagraphs (c) through (e) do not result in the employee disclosing classified information or other information contrary to law."

[2] Ibid.

[3] Ibid.

Gross Mismanagement
Case law developed under the WPA defines "gross mismanagement" as "a management action or inaction that creates a substantial risk of significant adverse impact on the agency's ability to accomplish its mission." The matter must be significant and more than minor wrongdoing or simple negligence. It does not include management decisions that are merely debatable among reasonable people.

Gross Waste of Funds
Case law developed under the WPA defines "gross waste of funds" as "an expenditure that is significantly out of proportion to the benefit reasonably expected to accrue to the government."

Substantial and Specific Danger to Public Health or Safety
Case law developed under the WPA holds that "substantial and specific danger to public health or safety" is determined by (1) the likelihood of harm resulting from the danger, (2) when the alleged harm may occur, and (3) the nature of the harm—the potential consequences.

Abuse of Authority
Case law developed under the WPA defines "abuse of authority" as "an arbitrary or capricious exercise of power by a military member or a federal official or employee that adversely affects the rights of any person or results in personal gain or advantage to himself or herself or to preferred other persons."

Urgent Concern

The Intelligence Community Whistleblower Protection Act of 1998 defines an "urgent concern" as any of the following:[2]
• 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 of the Federal Government that is—
  ○ a matter of national security; and
  ○ not a difference of opinion concerning public policy matters; or
• A false statement to Congress, or a willful withholding from Congress, on an issue of material fact relating to the funding, administration, or operation of an intelligence activity; or
• An action, including a personnel action described in section 2302 (a)(2)(A) of Title 5, constituting reprisal or threat of reprisal prohibited under section 407 (c) of the Inspector General Act of 1978, as amended, in response to an employee's reporting an urgent concern in accordance with this section.

Table 2.4.5.b. PPD-19 Personnel Actions

Personnel Actions
PART A: Retaliation in the Intelligence Community: • Appointment, promotion • Detail, transfer, or reassignment • Demotion, suspension, or termination • Reinstatement/restoration; reemployment • Performance evaluation • Decision concerning pay, benefits, or awards; or concerning education/ training that may reasonably be expected to lead to an appointment, reassignment, promotion, or performance evaluation • Decision to order psychiatric testing or examination Any other significant change in duties, responsibilities, or working conditions *Excluding any actions taken before July 8, 2013. See also PPD-19.F(4) and DTM 13-008 for a list of exclusions from the definition of "Personnel Action."*

2.4.6 PPD-19 Part B.

2.4.6.1 Persons covered by the directive. Any Executive branch employee eligible for access to classified information, including civilians, military members, and contractors.

2.4.6.2 Timeliness. Allegations of reprisal, under PPD-19 Part B, can be filed at any time; they are not subject to a time limit to file.

2.4.6.3 Reprisal analysis. Does the evidence, as supplemented by the interview of the complainant, make a *prima facie* allegation by including the following?

[2] See also 5 U.S.C. § 416(a)(2).

- Protected Disclosure or Activity. See Table 2.3.5.a. Does the evidence establish that the Complainant made a PD or was perceived as having made a PD; exercised any appeal, complaint, or grievance about a violation of Part A or B of PPD-19; lawfully participated in an investigation or proceeding about a violation of Section A or B of PPD-19; cooperated with or disclosed information to an IG, in general accordance with applicable provisions of law in connection with an audit, inspection, or investigation conducted by the IG; or reported a matter of urgent concern to Congress?

  See the definitions for PDs under Part A.

- Action affecting eligibility for access to classified information. Does the evidence establish that an Executive branch employee took, directed others to take, recommended, or approved any action affecting the complainant's eligibility for access to classified information?

- Knowledge/Contributing factor. Does timing or subject knowledge support that the alleged PD was a contributing factor in the action?

If these three factors above are present, the evidence supports a *prima facie* allegation of reprisal. However, the DoD OIG also evaluates any additional evidence collected during intake to determine if the facts and evidence warrant initiating an investigation, specifically the following.

- Causation. Do the facts support an inference of reprisal that warrants investigation? Evaluate whether all of the facts/evidence collected in the Intake phase suggest that the PD could have been factor in the action. Items to consider when assessing whether a causal connection exists between the PD(s) and the action include the following.

  - Temporal Proximity: The action followed closely behind the PD, or the timing and sequence of events indicates a PD could have been a factor in an action.

  - Motive: The PD was about something that would give the subject motive to reprise, or the subject has expressed animosity concerning the PD made by the Complainant.

  - Disparate Treatment: Was the Complainant treated consistently with other similarly situated nonwhistleblowers?

  - Strength of Available Evidence Supporting the action: Does the available evidence collected during the Intake phase clearly and convincingly establish that the basis for the action affecting the complainant's eligibility to access classified information was unrelated to the PD (no causal connection)?

2.5 WRI Intake Disposition Recommendations

The investigator analyzes the factors listed above and recommends to the SI whether the complaint makes a *prima facie* allegation that warrants investigation or whether other readily available facts/evidence clearly and convincingly establish that the action in question was taken for nonretaliatory reasons (no causal connection). *Prima facie* complaints of reprisal or military restriction may be referred to a Component IG for investigation. NAFI reprisal, contractor/subcontractor reprisal, and PPD-19 Part B cases may not be referred outside the DoD OIG for action. All decisions to dismiss complaints or for WRI to retain complaints for investigation require WRI Management, AI Front Office, or DoD IG approval.

2.6 Informing Chain of Supervision of High-Interest Matters

Investigators will promptly inform the ODIG AI chain of supervision of complaints that involve high-interest matters. High-interest matters are defined as those involving senior DoD officials, sexual assault, warfighter, public health and safety, congressional or news media interest, or other matters deemed to be of interest to the Secretary of Defense.

2.7 Notification of Initiation of an Investigation

2.7.1 Official Notification Correspondence. Once the determination has been made to open an investigation, the investigator will prepare official notification correspondence. The notification procedures may vary depending on the circumstances of the case. If a case involves a subject who is a senior official, the DIG AI will sign or initial the notification after orally notifying the subject of the investigation using the approved notification script.

2.7.2 ISO Case Notification. For ISO cases, the investigator will prepare a memorandum to the Component IG notifying them that the ODIG AI is opening an investigation into allegations against one of their senior officials. In some cases, the investigator will also prepare a memorandum to other DoD officials. The draft memorandum will be forwarded to the DIG AI or the IG for signature. The investigator will ensure the signed memorandum is placed in the case file.

2.7.3 WRI Case Notification. Consistent with the IG Act, whistleblower laws and regulations, and OIG confidentiality requirements, the investigator will prepare and coordinate notification correspondence making sure to not disclose the identity of complainants alleging reprisal or restriction or of witnesses to individuals outside of the DoD OIG unless an exception applies.

Handling Calls from Subjects. Investigators are the primary point of contact for subjects once an investigation is initiated. Investigators should encourage subjects to contact them directly (except for those cases in which the subject has legal representation, when communications with the subject must go through the subject's counsel), as any information provided by the subject to the investigator, SI, or other DoD OIG official will be considered part of the investigation.

CHAPTER 3—PLANNING INVESTIGATIONS

3.1 Investigative Plan

3.1.1 CIGIE Quality Standards. The first qualitative standard of the CIGIE "Quality Standards for Investigations," "Planning," requires an investigative organization to establish case-specific priorities and to develop objectives to ensure that individual tasks are performed efficiently and effectively.

All ODIG AI investigations require that an investigative plan be completed and approved before beginning fieldwork. ISO requires DIR/DDIR investigative plan approval. WRI requires SI investigative plan approval. The plans will be completed within established timeframes and as soon as possible after a determination is made to open an investigation. Investigators should schedule a roundtable discussion with the SI before beginning fieldwork. In ISO cases and in certain WRI cases as determined by management, the DIR/DDIR and the OGC attorney must also be present. Good investigative plans give investigators, supervisors, and attorneys a road map for conducting focused, thorough, and efficient investigations. As evidence is discovered and evaluated during the course of the investigation, investigative plans are often adjusted to maintain focus on relevant evidence and issues. Investigators will populate the required fields corresponding to the following elements in D-CATSe to build the investigative plan.

3.1.2 Key Elements of the Investigative Plan. The key elements of the investigative plan include:

- the subjects of the investigation;
- allegations or issues to be examined;
- applicable standards (laws, rules, or regulations) and the elements of proof for the standards;
- documentary and other relevant evidence to be collected;
- witnesses to be interviewed and questions relevant to allegation;
- the travel location and dates;
- investigation milestones; and
- investigative steps necessary to execute an organized, thorough, and efficient investigation.

3.1.2.1 Allegations/Issues. The first step in developing the investigative plan is to determine which allegations warrant investigation. This is probably the most important aspect of investigative planning. The investigator will consult with the assigned attorney to be certain the issues that warrant investigation are correctly identified based on the information contained in the complaint and gathered from the complainant. This is necessary to properly focus the investigation and avoid unnecessary or unproductive investigative activity.

3.1.2.1.1 In senior official cases, this will involve a determination of issues that the investigation will address and a prioritization of those issues based on whether they constitute a credible allegation of serious misconduct, or if they will not be investigated because they lack investigative merit. Some of the more common reasons for not investigating an issue include:

- the allegations do not contain enough specific detail to be actionable;
- the allegations, if true, would not constitute a violation of a law, rule, or regulations;
- the allegations involve issues that are more properly addressed in other channels (EEO, administrative grievance, management officials/chain of command);
- the allegations involve actions or events that occurred many years ago and are too old to investigate; and
- the allegations involve matters that are minor and, therefore, an investigation would not be a prudent use of limited Government investigative resources.

These determinations must be made in coordination with the supervisor, DDIR, and DIR.

3.1.2.1.2 In reprisal cases, the determination will involve identifying all alleged protected communications or disclosures and the personnel actions that will be included in the scope of the investigation, as well as evidence needed to establish the elements of subject knowledge and causation. Those allegations that meet the *prima facie* determination will be investigated.

3.1.2.2 Standards/Statutory Authorities. Investigators need to thoroughly research and understand the applicable laws, rules, or regulations early in their investigation planning. This means not only understanding which particular standard applies, but also understanding the applicable language in the standard that needs to be proved or disproved (elements of proof) for a violation to have occurred. Keep in mind that different reprisal statutory authorities employ different standards of proof. Correctly developing issues and standards leads to the selection of the best witnesses to interview, the questions to ask the witnesses, and the documents to obtain.

To facilitate the standards research process, investigators should refer to the ODIG AI SharePoint site. Links can be found to the most commonly used regulations for ODIG AI investigations. Templates are also available for most commonly used standards to facilitate incorporation into the investigative plan and later into the report of investigation (ROI).

Investigators should remember the following when researching standards.

- Ensure that the standard was in effect at the time of the events under investigation.

- Research regulations that apply at the Federal level, DoD level, Military Department level, and Command level, as well as policy memorandums and manuals. Discuss with the OGC which standard governs or is controlling with respect to the issues under investigation.

- Pay close attention to standards that apply to combatant commands, Joint organizations, or international alliance organizations such as the North Atlantic Treaty Organization.

3.1.2.3 Biographical and Organizational Data. Investigators should perform research and become knowledgeable on the people and organizations involved in the investigation as a fundamental step in preparing for interviews and obtaining evidence. Whenever possible, investigators should review documents that show the organizational structure and the chain of command. They should know the mission and function of the organization before interviewing its members. This will help place in context the information provided by witnesses. Similarly, investigators should review individual biographies (most common with senior officials) and personnel records to help develop pertinent questions for each witness.

3.1.2.4 Documentary Evidence. It is important for investigators to identify in the planning phase any and all documentary evidence to be obtained during their investigation.

3.1.2.4.1 Access to Records and Information. Under DoDD 5106.01 and DoDI 7050.03, "Office of the Inspector General of the Department of Defense Access to Records and Information," March 22, 2013 (Incorporating Change 1, Effective April 24, 2020), DoD OIG investigators are to be granted expeditious and unrestricted access to copies of all records, regardless of classification, medium (for example, paper and electronic) or format (for example, digitized images and data) and information available to or within any DoD Component. No officer, employee, contractor, or Service member of any DoD Component may deny the DoD OIG access to records.

Accordingly, investigators should consider the following.

- Documents. Investigators should identify the types, sources, and locations of documents to be collected. In cases that require gathering a large volume of documents or using a subpoena, good planning provides the opportunity to initiate formal written requests for records early in the investigation and may avoid delays when the investigation is at a critical stage.

- E-mail. Obtaining e-mails is an important and fundamental step in conducting investigations. Investigators should work through IG offices or other designated points of contact to reach the appropriate systems administrator personnel. Investigators should start with an initial phone contact, and then provide a written request identifying specific e-mail accounts (that is, non-classified Internet protocol router [NIPR] or SECRET Internet protocol router [SIPR] network) required, and include the IG Act and IG Access to Records authorities in the written request.

3.1.2.4.1 Types of Records. The procedures below should be followed to obtain special types of records:

- Personnel Records. Military personnel records are maintained at personnel centers for the Military Departments. Investigators should contact the following offices to obtain military personnel records:
    - Army personnel: United States Army Human Resources Command (HRC) Inspector General
    - Navy: Bureau of Naval Personnel (BUPERS) Inspector General
    - USMC: Headquarters United States Marine Corps Manpower and Reserve Affairs
    - Air Force: Air Force Personnel Center (AFPC) Inspector General
    - Space Force: Air Force Personnel Center (AFPC) Inspector General

  Coast Guard: Director of Military Personnel

  Civilian personnel records may be maintained at agency or command human capital or human resources offices.

- Contract Records. The Contracting Officer or the Contracting Officer's Representative (COR) are the fastest and most efficient source for obtaining contract documents. In the absence of contact information for the Contracting Officer or COR, the Defense Contract Management Agency (DCMA) or the Defense Contract Audit Agency (DCAA) can provide assistance. If the contract relates to a specific DoD facility or installation, a local contracting office may be able to provide information. The local IG can also help locate the points of contact at the installation. Contract information and documentation can be obtained from several DoD and Federal systems. The Federal Data Procurement System (FPDS) can be searched by company or DoD organization name to obtain contract numbers, and the Electronic Document Access (EDA) system can be searched using the contract number to obtain contract documents.

- Travel Records. The Defense Finance and Accounting Service (DFAS) is the central repository for disbursements for official travel. To obtain travel records, investigators should submit a written request on letterhead to the Defense Finance Accounting System Internal Review, Criminal Investigations Branch, with the following information.
    - The document requested (such as a voucher, order, or receipt)
    - The traveler's full name, Social Security number , and travel date range

- Where the voucher was most likely filed or processed
- Whether the voucher was filed under the Defense Travel System (DTS)

3.1.2.5 Witnesses. Under DoDD 5106.01, DoD OIG investigators are authorized to obtain statements from DoD personnel on matters that the DoD IG considers appropriate for investigation. To the extent possible, investigators should identify all of the witnesses to be interviewed in the investigation during the planning phase. At a minimum, identify witnesses by their titles or relationship to the complainant or the subject. The earlier information is identified, the better the investigator can plan the course of inquiry. Organizational charts help identify the titles and ranks of witnesses and where they fall in the chain of command.

3.1.2.5.1 Witness Availability. Once witnesses are identified, investigators should determine their current duty assignments and availability. This is important in planning because witnesses may have been given temporary duty assignments, transferred, resigned, or retired since the time the alleged misconduct occurred. Witness availability can determine the order of witness interviews and the timing of the investigator's travel.

3.1.2.6 Travel Locations and Dates. Investigators should plan travel in the most cost-effective manner. In cases that involve multiple witnesses in multiple geographic locations, careful planning, coordination, and timing is required. To the extent possible, investigators should combine travel to several different locations into one trip within the same geographic area. Instead of long distance travel for one interview, they should consider alternatives such as the use of video teleconferencing, web camera technology, or telephonic interviews.

3.1.2.7 Investigative Steps. The investigative plan should reflect the strategy or the steps through which the investigator plans to proceed to complete the case. The investigator should consider the order of the witness interviews, the documents to obtain, and any special investigative aids or methodologies that may be employed—for example, the issuance of a subpoena. The investigator should develop a course of action that will maximize efficiency and effectiveness. However, the investigator should not become locked into the plan; he or she should continually assess the progress of the inquiry and adjust the plan accordingly.

3.1.2.8 Investigative Milestones. Investigative milestones should be established and entered into D-CATSe during investigative planning. The milestones should be consistent with the priority of the investigation or the statutory or regulatory timeframes. The milestones should be established through the planned case closure date allowing time for supervisory and OGC review. Investigators should work rigorously to meet the established milestones. Once entered in D-CATSe, the planned milestones should not be changed, and the actual milestones should be entered. If processing delays occur during the investigation, such as waiting on records, investigators should document the reason for the delays in D-CATSe.

3.1.3 Investigative Roundtables. In addition to the investigative planning roundtable, investigators should schedule roundtable discussions with the SI. In ISO cases, and in certain WRI cases as determined by management, the DIR/DDIR, and the OGC attorney must also be present to discuss the facts, draft ROI, and next steps in the investigative process. The roundtable discussions serve as the mechanism for facilitating the interactive, write-as-you-go investigative process. D-CATSe is used in these meetings for participants to access all information pertaining to a case. At

a minimum, roundtable discussions should be conducted just before the subject interview (pre-subject) and after the subject interview (post-subject) to collaborate on case-related information.

3.2 Onsite Fieldwork

3.2.1 Preparation. Investigators should obtain and review as much of the documentation and e-mails as possible before onsite travel to help with selecting witnesses and developing interview questions. At least 10 days before arriving onsite, investigators should make necessary local arrangements to ensure the onsite fieldwork is effective and efficient. The local IG is normally best suited to help with DoD OIG investigations. They can help arrange interviews, interview locations, and access to witnesses. Most importantly, investigators should ensure that the complainant, the subject, and key witnesses will be available.

3.2.2 Travel Logistics. Investigators will need to obtain authorization for certain logistics before their travel.

3.2.2.1 DTS and Travel Standards. Investigators must arrange and obtain authorization for their travel in the DTS. Investigators need to review the DTS pre-audits and address those matters that require justification and authorization in accordance with the Joint Travel Regulations and other DoD travel standards. Use of the Government travel card is mandatory for all expenses related to official travel. Vouchers must be submitted within 5 days of return from a trip.

3.2.2.2 Foreign Travel. Investigators must report all planned official foreign travel to the Office of Security. Consult the "DoD Foreign Clearance Guide," DoD OIG Security, and DoD OIG Overseas Contingency Operations (OCO) to determine the need for official passports, visas, theater clearance, NATO orders, country clearance, country briefs, advance notifications, and security clearances. Most DoD OIG travel support offices require 30-day advance notice of overseas travel and longer if official passports and visas are involved. Investigators may also need to complete DoD and Agency training requirements related to overseas travel.

3.2.2.3 Travel Compensatory Time Request. If travel is expected to exceed normal business hours, the investigator must complete a request for travel compensatory time within 5 days of returning from the trip.

3.3 Investigative Tools

As part of the investigative process, investigators may find it helpful to use one or more tools that can help organize the investigation and the analysis of the evidence. Offices may use computer-based tools to help organize and analyze evidence. Other static or written forms of such tools include the following.

3.3.1 Investigation Matrix. An investigation matrix (Table 3.1) is helpful in organizing the witnesses who need to be interviewed for each allegation addressed by the investigation.

Table 3.1. Investigation Matrix

Witness	Allegation #1	Allegation #2	Allegation #3	Requested Document
Mr. Jones (Confidential Complainant)	X	X	-	
Col Smith	X	~	-	
(Chief of Staff)	X	~	-	
RADM Shipless (Commander)	~	~	-	
Mr. Boomer (Coworker)	~	~	-	
Mr. Spock	X	X	X	
(Coworker)	X	X		Was a safety report filed? Was leave requested?

Legend:
X Primary witness
- Discuss if knowledgeable
~ Do not discuss
Source: The DoD OIG.

CHAPTER 4—CONDUCTING INVESTIGATIONS

4.1 Introduction

The nature of administrative investigations presumes that the allegations under investigation, if substantiated, are not reasonably expected to result in criminal prosecution. If, during the course of conducting an administrative investigation, the investigator discovers evidence of potential violations of criminal law, the investigator should discuss the evidence with his or her supervisor. Together, they should determine whether additional investigative activity should stop and they should notify the DoD OIG Defense Criminal Investigative Service (DCIS).

4.2 Professional Quality Standards

4.2.1 Basic Standard for Execution. The CIGIE qualitative standards for the execution of investigations directs investigators to conduct investigations in a timely, efficient, and thorough manner that meet legal requirements. It notes that the investigator is a fact-gatherer and should not allow conjecture, unsubstantiated opinion, or bias to affect work assignments. It also notes that investigators have a duty to be receptive to evidence that is non-incriminating as well as incriminating.

4.2.2 Objectivity. Investigators must always remain objective and conduct themselves with the highest degree of professionalism, integrity, and impartiality, approaching each case without prejudging people or reaching predetermined conclusions.

4.2.3 Thoroughness. In exercising due professional care and for investigations to be credible, investigators must be thorough. In general, they should interview all material witnesses and obtain all evidence relevant to the issues under investigation. Investigators should be especially careful to pursue witnesses and documents identified by the subject and complainant. Taking shortcuts can result in more work in the long run and may undermine the credibility of the investigation and the DoD OIG. Investigators should routinely assess the evidence they have obtained during the course of their investigations and consult with their supervisors about emerging allegations, whether they have obtained sufficient evidence, and whether to continue or terminate the investigation.

4.2.4 Timeliness. Investigators must conduct investigations in a timely manner. This means accomplishing investigative activities with a sense of urgency and with all due regard for statutory timeframes, established deadlines, and organizational performance metrics. Investigators should focus on the issues and the scope identified in the investigative plan, and discuss with their supervisors how to handle new issues raised during the course of the investigation. Investigators must remember that the investigations they conduct can have a profound effect on individuals' lives, professional careers, and reputations, and on the activities of organizations.

4.2.5 Team Approach. The ODIG AI administrative investigative process is based on the team concept. Peer, supervisory, and legal participation in the investigative process expand and build on individual investigator expertise. As the finished product is the report of the DoD IG, not the investigator, the team approach employs the collective talent, expertise, and intellect of the ODIG AI and the OGC to deliver the best possible product. This approach helps the investigator resolve complex matters and minimizes the potential for individual bias.

4.2.6 Write-as-you-go. Once fieldwork begins, the investigation follows an iterative cycle in which the investigator continuously assesses information gaps, accumulates additional information to address those gaps, analyzes the information relative to applicable standards, and drafts the ROI. Investigators use this "write-as-you-go" methodology to substantially complete major portions of the ROI during fieldwork. This is an established investigative best practice that significantly contributes to a thorough, timely, and complete investigation.

4.3 Elements of the ODIG AI Investigative Process

All ODIG AI investigations will employ the elements of the investigative process as set forth below.

4.3.1 Official Notifications. Official notifications regarding the initiation of an investigation will be made to the subjects, Military Departments Inspectors General, and DoD Components as deemed appropriate in each case. Notifications may be delayed if determined to adversely impact the investigation. Notification templates are located on the AI SharePoint site.

4.3.2 Confidentiality. Confidentiality will be provided to complainants and sources of information to the fullest extent permitted under the law.

4.3.3 Privacy. Information relating to investigations will be safeguarded out of respect for individual privacy and professional reputations as required by the Privacy Act and guidance on official use information. Investigators will not discuss ongoing or past investigative work with individuals who have no official need to know such information. All media inquiries will be referred, without comment, to the OLAC Director.

4.3.4 Sworn Recorded Testimony. Sworn recorded testimony will be obtained from complainants, witnesses, and subjects with firsthand knowledge of the events at issue.

4.3.5 Complainant Interviews. The complainant (if known) will always be interviewed; the complainant will usually be interviewed first to clarify allegations and issues.

4.3.6 Subject Interviews. The subject of the investigation will always be interviewed. This gives the subject the opportunity to tell his or her side of the story, respond to the allegations made against him or her, and identify witnesses and evidence that may be material to the matters under investigation.

4.3.7 Documentation. Investigative findings and activities will be fully supported with accurate and complete documentation in the Evidence and Report References folder in the case file. All evidence relied on in the ROI will be included in the D-CATSe Report References folder.

4.3.8 Quality Controls. Quality controls will be in place, including referencing source documents to facts in investigative reports, management reviews of reports, and supporting evidence.

4.3.9 Legal Review. The OGC will perform a legal sufficiency review of every final ROI to ensure supportability of the findings and conclusions.

4.3.10 Tentative Conclusions. Subjects will typically be notified (either orally or in writing) of tentative conclusions where allegations are substantiated, and they will be given an opportunity to respond to the tentative conclusions before the OIG issues the final report.

4.3.11 Final Reports. Final reports will be provided to management officials or complainants as warranted. The release of the reports will be accomplished consistent with the guidelines for protecting identities and the privacy of complainants, witnesses, and subjects under the IG Act, Privacy Act, and Freedom of Information Act.

4.3.12 Closure Letters. Closure letters will be provided to subjects, complainants, Military Departments Inspectors General, Component-designated officials, and other officials required by statute or directive, as appropriate, with the conclusions of the investigation upon completion.

4.4 Documentary Evidence

4.4.1 Obtain All Relevant Documentary Evidence. An investigator should obtain all relevant documentary evidence. If facts or events are documented, the investigator should obtain copies. Examples of relevant documents include personnel records, travel records, contract records, pay records, security records, internal memorandums, calendars, and policy and regulatory documents. An investigator should consider obtaining e-mails in every investigation, as they have proven to be valuable contemporaneous evidence in documenting actions or events.

An investigator should not request documents before visiting an organization if concerned that the request would result in the destruction of critical evidence or otherwise compromise the investigation. Under such circumstances, an investigator should go to the location of the documents, request the documents from the appropriate management official, and observe the retrieval of the documents. In general, it is acceptable to take copies of documents, leaving the originals with the organization.

4.4.2 Documentary Evidence Is Often the Best Evidence. Contemporaneous documents are frequently more reliable than testimony, particularly for events that occurred months or years earlier. In some cases, a single document may constitute direct evidence of wrongdoing. In other cases, investigator should build a strong foundation for substantiating or refuting an allegation with documentary evidence, and then build on that foundation with witness testimony.

4.4.3 Take a Copy. If doubts arise regarding the ultimate relevance of a document, it is usually best to obtain a copy of the document. As an example, local command instructions, whose value may not be readily apparent during an investigator's onsite work, may later provide insight in identifying systemic problems in certain cases.

4.4.4 Examples of Relevant Documents

4.4.4.1 Adverse Personnel Action Cases. Examples of documents that are helpful in investigations of whistleblower reprisal for prohibited personnel practices include official personnel files, performance evaluations, merit promotion and selection documents, medical and mental health evaluation records, EEO or grievance records, records of non-judicial punishment proceedings, and other formal and informal disciplinary action records. These records are located at the civilian or military personnel offices, EEO or social actions offices, medical facilities, and within supervisory and administrative files.

4.4.4.2 Abuse of Official Travel Cases. Records that are helpful in investigations related to the abuse of official travel include travel orders, vouchers, itineraries, calendars, and visitor logs. They may be found within finance or payroll centers and headquarters administrative files. In cases involving alleged misuse of military aircraft (MilAir), requests for MilAir, flight

advisory messages, and passenger manifests may be obtained from the Joint Operational Support Airlift Center, Scott Air Force Base (AFB), Illinois, or the aviation unit flying the mission in question.

4.4.4.3 Improper Contracting or Funding Cases. In cases involving improper contracting or expenditure of funds, helpful records include contracts, modifications, specifications, performance work statements, statements of work, proposals, source selection criteria, DD Forms 448, "Military Interdepartmental Purchase Request," and documents reflecting budget decisions, such as minutes from organization Program and Budget Advisory Committee meetings. These documents can be found in the local contracting officer's files, contracting officer's technical representative's files, program management files, finance or budget office files, and the servicing DFAS office records.

4.4.4.4 Previous Investigations. If the command has previously investigated the matters under investigation, such as a local IG inquiry or commander's inquiry, an investigator should obtain a copy of the report and underlying documentation and also interview the investigating officer.

4.4.4.5 Obtaining Information from Computers. As a general rule, information stored in Government computers and information systems is considered Government property. Similarly, e-mail—that is, .pst files—and other electronic documents are official records. All DoD systems are required to have official logon warning banners advising employees and other authorized users that the systems are subject to monitoring. An investigator should ensure the standard DoD banner is displayed on the Government information system when obtaining records from that system. DoD employees do not have a reasonable expectation of privacy with regard to the communications or documents they transmit on DoD systems.

An investigator should contact his or her supervisor and the OGC in situations in which there is a concern about a particular system or in situations in which files are password-protected separately from other files.

4.4.5 Requesting Records

4.4.5.1 Telephonic and E-Mail Requests. An Investigator may request documents through a telephonic or e-mail request to expedite delivery of the documents. Telephonic or e-mail requests for records may be made to the Military Department or agency point of contact (POC) or directly to the organization in possession of the records. The investigator should follow a telephonic request with an e-mail to confirm the documents or information that is needed and to provide a written record of the request.

If an individual is reluctant to respond to an initial request because he or she wants to verify the investigator's identity, the investigator has several options.

- Refer the individual to the Military Department or local IG, who can confirm that the investigator is a representative of the DoD IG.

- Advise the individual to call the DoD Hotline, 1-800-424-9098, for a DoD Hotline investigator to confirm the investigator's identity.

- An investigator should coordinate with the DoD Hotline so the call is expected. The investigator may also fax a business card to the individual.

Note: An investigator should never copy or fax his or her credentials.

4.4.5.2 Formal Written Requests. In many instances, an investigator should send a formal written request for documents on official DoD IG letterhead. This is preferable in significant cases in which it is important to set the tone with the Command or the organization that the DoD IG is formally investigating, establish a formal written request of the documents that are requested, and set the suspense date for provision of the documents.

Requests for records will include the following language:

> This request for records is made in conjunction with an official investigation being conducted by the DoD Office of Inspector General. The request is made under the authority of DoD Directive 5106.01, "Inspector General of the Department of Defense (IG DoD)," April 20, 2012 (Incorporating Change 2, Effective May 29, 2020), paragraph 7.b., which states that the IG DoD will have access to "all records (electronic or otherwise), reports, investigations, audits, reviews, documents, papers, recommendations, or other information or material available to any DoD Component."

4.5 Access to Records

4.5.1 Authority

4.5.1.1 The IG Act. The IG Act provides that each IG is authorized:

> to have access to all records, reports, audits, reviews, documents, papers, recommendations, or other material available to the applicable establishment which relate to programs and operations with respect to which that Inspector General has responsibilities under this Act.

4.5.1.2 DoDD 5106.01. DoDD 5106.01, paragraph 7.b., delegates to the IG the same access to items as in the IG Act, as quoted above, specifying that records may be "electronic or otherwise."

4.5.1.3 DoDI 7050.03. DoDI 7050.03, "Office of the Inspector General of the Department of Defense Access to Records and Information," March 22, 2013 (Incorporating Change 1, April 24, 2020).

Paragraph 3.a. of this Instruction sets forth as a matter of policy that:

> The OIG DoD must have expeditious and unrestricted access to all records, regardless of classification; medium, such as paper or electronic; or format, such as digitized images or data, and information available to or within any DoD Component.

> Paragraph 3.b. establishes as policy that:
>
> No officer, employee, contractor, or Service member of any DoD Component may deny the OIG DoD access to records. Only the Secretary of Defense can deny access to certain types of records or information based on criteria listed in DoDD 5106.01, paragraph 6a(1), relating to operational plans; intelligence; counterintelligence; criminal investigations involving national security; and other matters, disclosure of which would constitute a serious threat to national security.
>
> Enclosure 2, Paragraphs 2.a. and 2.b., directs that DoD Component heads must:
>
> Establish procedures to ensure that requests for access to records or information under authorized DoD OIG audit, investigation, followup, or oversight projects are granted immediately, or that objections requiring action by the Secretary of Defense regarding the release are submitted in writing to the DoD IG by the Component head no later than 15 business days from the date of the DoD OIG request.

4.5.1.4 If an individual resists the DoD OIG's authority for access to information, the investigator should advise the individual that he or she should contact the local IG or staff judge advocate to confirm the DoD OIG authority. In the event that the investigator cannot resolve the denial of access at the local level, he or she should immediately notify his or her supervisor, who will resolve the matter at the level of command necessary to obtain the required access.

4.5.2 Classified Information

4.5.2.1 Introduction. Access to classified information is governed by the Inspector General Instruction 5200.1, "Information Security Program," August 20, 2018, which implements DoD Manual 5200.0l-R, "DoD Information Security Program," February 24, 2012 (Incorporating Change 2, July 28, 2020).

4.5.2.2 Need to Know. Before granting the investigator access to classified information, the possessor of the classified information must first determine that the investigator is required to access the classified information for lawful and authorized Government purposes. In most instances, this "need to know," will be self-evident from the fact that the investigator is conducting the investigation pursuant to the authority conveyed to the DoD IG by the IG Act and DoDD 5106.01.

4.5.2.3 Security Clearance. Classified information may be disclosed to the investigator by the possessor of the classified information only after a determination has been made that the investigator has the appropriate clearance to receive the classified information. If verification of the security clearance is requested, the investigator should contact the Office of Security.

4.5.2.4 Transporting Classified Information. An investigator should not transport classified material unless authorized to do so as delineated by a courier card. Instead, an investigator should contact a supervisor to coordinate transportation of classified documents by personnel granted a courier card by the Office of Security. Outside the Continental United States (CONUS), an investigator should have the local security officer contact the Office of Security to coordinate the delivery of classified documents.

4.5.2.5 Safeguarding Classified Information. When required to review classified documents or include classified information in an ROI, it is imperative that an investigator follow the rules governing protection and accountability of classified information. Classified information must be afforded the level of protection against unauthorized disclosure commensurate with the level of classification assigned—that is, confidential, secret, or top secret.

Policy and procedures regarding the marking, safekeeping and storage, access, dissemination, accountability and control, transmission, and disposal and destruction of classified information are discussed in detail in DoD Inspector General Instruction 5200.1.

4.5.3 Obtaining Special Access Program Information. Access to special access program (SAP) information will be determined on a case-by-case basis and limited to the minimum necessary to perform the functional requirements under DoD Inspector General Instruction 5205.07, "Special Access Programs," February 13, 2020, and DoDD 5205.07, "Special Access Program (SAP) Policy," July 1, 2010 (Incorporating Change 2, February 4, 2020).

4.5.4 Non-DoD Government Records and Records of Other Federal Agencies. The IG Act authorizes the DoD OIG to request information or assistance from other Federal agencies as may be necessary for carrying out DoD OIG duties and responsibilities. Requests for documents in ODIG AI administrative investigations from another Federal agency should be made through that agency's IG. The names and telephone numbers of more than 60 statutory and administrative IGs can be obtained from the directory published by CIGIE, which is maintained by the DoD, Principal Assistant Inspector General for Audit. IG data is also available on the Internet at http://www.ignet.gov/.

4.5.5 Non-Government Records and IG Subpoenas. During the course of an investigation, it may be necessary to obtain records from private individuals, corporations, partnerships, nonprofit organizations, and other non-Federal government entities. To obtain these documents it may be necessary to issue a DoD IG subpoena. A DoD IG subpoena can require banks, credit unions, and credit card companies to turn over financial records including customers' bank statements, checks, deposit slips, and safety deposit records. An IG subpoena can also be used to require hotels to release lodging records, phone companies to release phone records and text messages, and airlines to release ticketing records. An IG subpoena can also require state and municipal governments to turn over documents. The process for obtaining an IG subpoena is administered by the DoD OIG OGC. Investigators should refer to the DoD OIG website for guidance and templates for obtaining an IG subpoena (https://www.dodig.mil/Programs/Subpoena-Program/).

4.6 Experts and Other Sources of Assistance

4.6.1 Introduction. When used effectively, assistance from experts and other sources can enhance the credibility of investigations and provide the critical element needed to prove or disprove the allegations. Investigators should consider obtaining assistance from a variety of experts outside of ISO and WRI when necessary. They should consult with their supervisors before seeking this type of assistance.

4.6.2 Technical Experts

4.6.2.1 DoD Policy Experts. In cases where Military Department regulations are unclear or appear to conflict with DoD regulations, investigators will work with the OGC to obtain a

clarification of the correct policy to be applied in their case. The OGC may seek a policy interpretation from the policy experts in the DoD proponent office responsible for the directive, instruction, or policy memorandum. In those situations, investigators will need to provide sufficient detail regarding the facts of their case and the regulations that are potentially applicable. It is helpful to provide this information in writing to help the OGC render an opinion in the matter.

4.6.2.2 Medical Experts. Numerous physicians, psychiatrists, and psychologists are located at local Air Force, Army, Navy, and Marine Corps installations. The DoD IG has access to the Surgeons General of the Military Departments and the Office of the Assistant Secretary of Defense for Health Affairs, as well. These physicians may serve as consultants and expert witnesses, or may be asked to provide their opinion about a medical report or diagnosis. Normally, a written request is required outlining the need for the physician in connection with an investigation.

4.6.2.3 Engineers. Engineers are helpful in cases requiring the analysis of extremely technical or scientific information. Engineers who can help with investigations are assigned within the Office of the Deputy Inspector General for Policy & Oversight, Technical Assessment Directorate.

4.6.2.4 Auditors. Auditors are available from the ODIG AUD (Audit). Additionally, each Military Department has auditing organizations that may provide assistance. The Defense Contract Audit Agency is responsible for the audit of pricing and costs related to DoD contracts within the DoD, and may be used to conduct audits of invoices, billings, and costs charged to contacts.

4.6.2.5 Safety Experts. Expertise in the various safety functional areas (for example, flight safety or explosive safety) may be obtained from the safety centers of each Military Department: Army Safety Center, Fort Rucker, Alabama; Air Force Safety Center, Kirtland AFB, New Mexico; or Naval Safety Center, Norfolk, Virginia.

4.6.2.6 Computer Support

4.6.2.6.1 Technical support for obtaining and analyzing evidence stored on removable media or hard drives is available from the Technical Services Directorate of DCIS. Specialists can perform mirror imaging and forensic analysis of hard drives and servers, and may be able to recover data that was deleted from a hard drive or reformatted on removable media.

4.6.2.6.2 If a case is especially data intensive, certain database programs may greatly aid in the storage, recovery, and analysis of evidence and information. Assistance may be obtained from the Office of the Chief Information Officer.

4.7 On-Site Field Work

4.7.1 Arrival On Site. On arrival at the activity, the investigator should visit the local POC and ensure satisfactory arrangements have been made for witness interviews, records retrieval, and administrative and logistical support. The investigator should check the facility provided for interviews and ensure that it is private and adequate (for example, that it has sufficient tables and chairs, as well as an electrical outlet for the recorder).

4.7.2 Thoroughness On Site. Investigators should not conclude the onsite visit until they conduct a thorough investigation. Investigators should interview new witnesses who have been identified during the course of the visit and are available locally. Similarly, investigators should

take the time to review documents that are identified to ensure that valuable new evidence is not overlooked. In reprisal cases, particularly if the complainant's interview was telephonic before a site visit, an investigator should try to meet with the complainant face-to-face, if feasible, to ask followup questions arising from newly obtained testimony or investigative leads. If necessary, an investigator should extend his or her travel rather than skip logical investigative leads or make a second trip to the same location.

4.7.3 Out-Briefings. If the local commander requests an out-briefing, investigators should express appreciation for support received and limit the conversation to a general discussion of the investigative process and the progress made while on-site. However, investigators will not speculate on findings and conclusions of the investigation, and will also avoid giving a date that the investigation will be completed. Instead, investigators may inform the commander about the investigative process, which involves a rigorous review process including quality assurance and legal reviews before approving and issuing the report of investigation.

CHAPTER 5—INTERVIEWS

5.1 Introduction

5.1.1 Professional Conduct. One of the keys to the successful resolution of investigations rests with the ability of the investigator to elicit information from witnesses during interviews. How investigators conduct themselves and how well they are prepared sets the stage for the interview process. Investigators should conduct themselves at all times in a manner that reflects the highest standards of integrity, impartiality, and competence. To maintain the credibility of the DoD IG and ODIG AI, investigators must conduct themselves in keeping with professional standards.

5.1.2 During Interviews

5.1.2.1 Be Objective. Investigators should approach interviews with an open mind. Investigators should ask questions to get both sides of the story—non-incriminating and incriminating information. Investigators should not lead witnesses by asking questions designed to reach a preferred answer, but should let the witnesses tell their side of the story.

5.1.2.2 Be Prepared. The investigator should know the objective of the interview. The investigator should know what information needs to be obtained from the interview, and the standards and the elements of proof for the conduct in question. The investigator should prepare a list of questions before the interview to thoroughly elicit the needed information.

5.1.2.3 Listen. Investigators should ask short, direct, open-ended questions and listen to the answers. Investigators should give witnesses a chance to answer questions and not interrupt, not do all of the talking, and let witnesses talk about their knowledge of the events under investigation.

5.1.2.4 Be Respectful. Investigators should treat witnesses with dignity and respect. The investigator should treat a witness with the same respect that the investigator would like to receive if he or she were the one being interviewed. The investigator should not be rude or condescending. It is permissible to challenge or confront a witness but not to berate, coerce, or harass the witness.

5.2 Interview Process

5.2.1 Planning. It is imperative that the investigator is well prepared before interviewing witnesses. This requires planning. First, the investigator should identify all relevant issues and elements of proof. Next, the investigator should consider the facts or information necessary to resolve each of those issues. Then the investigator should determine which witnesses can supply needed facts or information and, thus, must be interviewed. Next, the investigator should formulate an objective for each interview and develop a line of questioning based on that objective. Then the investigator should consider the location of the interviews and the order in which witnesses will be interviewed. Finally, the investigator should review the complaint, biographical data on the witnesses, files and documentary evidence (such as .pst files), and information on the witnesses' organizations.

5.2.2 Selection of Witnesses to Interview. When conducting an investigation, the investigator should always interview the complainant, the subject, and other primary witnesses (those having firsthand knowledge of the events at issue). The investigator should interview witnesses identified by the complainant as well as those identified by the subject. Failure to interview primary witnesses can lead to insufficient fact-gathering and unfounded conclusions, and may undermine the credibility of the DoD IG to conduct thorough investigations.

However, investigators may not need to interview all of the witnesses identified by the complainant or subject. Some interviews may be redundant and serve no probative purpose. For example, if five witnesses have clearly established a fact, it is not necessary to continue interviewing witnesses on the same point. On the other hand, investigators should not avoid witnesses who may have valuable information. When in doubt, investigators should perform a screening interview to determine if the witness has pertinent information about the matter under investigation. If the witness has information needed to complete the case, the investigator should proceed with a sworn recorded interview.

5.2.3 Objective of Interview. Before conducting an interview, the investigator should know what evidence the witness can be expected to provide. Before the interview, the investigator should determine what information that witness may possess that will either substantiate or refute the allegations and develop a line of questioning designed to obtain that information.

5.2.4 Line of Questioning. Under most circumstances, the investigator should prepare a list of questions, or interrogatory, to ask a primary witness before conducting the interview. The investigator should anticipate possible responses and formulate followup questions. This process will focus attention on the interview beforehand, resulting in increased confidence and control during the interview itself.

Aside from the scripted read-in and read-out, the investigator should avoid getting locked into a prepared script. During the interview, the investigator should ask a question, listen to the answer, consider the objectives and areas of interest, and go with the flow of the testimony. Nonetheless, it is paramount that a witness addresses all the areas of concern. The investigator should be prepared with an outline of "must ask" questions to ask, if necessary.

5.2.5 Location of Interviews. The location of the interview should be compatible with the confidentiality of an Inspector General inquiry. If possible, the investigator should conduct interviews in a quiet location away from the witness's office to ensure privacy and prevent interruption. The atmosphere of privacy helps place witnesses at ease and makes witnesses more forthcoming. A quiet location reduces distractions and enhances the quality of the recording.

- Investigators should consider conducting interviews in designated interview rooms. When on travel, the local IG or POC can frequently provide an interview room or conference room that provides privacy. If it is difficult to find an adequate interview site, the investigator should contact the legal offices (staff judge advocate or general counsel) and request assistance.

- As a matter of courtesy, investigators will normally interview senior officials in their offices. The investigator should coordinate in advance with the senior official's executive officer, aide-de-camp, or secretary to ensure that the senior official is informed that a private, sworn, recorded interview will be conducted and that the interview is not to be interrupted.

- Complainants and other witnesses frequently will not want to be interviewed in their workplaces or during duty hours. Some witnesses will be fearful of retaliation if they are seen speaking to a DoD OIG investigator. If necessary, the investigator should arrange to interview those witnesses after duty hours at off-post locations, such as public buildings, Government offices, hotel rooms, or private residences. Two investigators should always perform interviews in hotel rooms or private residences.

- Telephone interviews may be used with witnesses or when circumstances make an interview in-person impossible, unduly expensive, or time-consuming. When conducting a telephone interview, the investigator should take steps to ensure that the witness has sufficient privacy to discuss the issues candidly.

5.2.6 Scheduling Interviews. Unless completely impractical, the investigator should initiate contact with a witness via phone call. The investigator should explain AI policy about swearing in, recording, and transcribing interviews, and using two interviewers. The investigator should introduce the Privacy Act notice and get the witness's e-mail address. The investigator should not rush interviews, particularly those with the subject or the complainant. The investigator should schedule interviews to allow sufficient time to cover all the issues and allow enough time to follow up on unanticipated information. The investigator should allocate time for breaks (generally 5 or 10 minutes each hour). The investigator should schedule appointments with sufficient time between them so the witnesses do not encounter one another when arriving at or leaving the interview site. The investigator should follow up the phone conversation with an e-mail confirming the time and location of the interview and attach the Privacy Act notice**.** When scheduling multiple interviews at a remote location, the investigator should consider having the local IG provide a scheduling POC to best fill your time.

5.2.7 Biographical and Organizational Data. Investigators should perform research and become knowledgeable on the people and organizations involved in the investigation in preparing for interviews. Whenever possible, investigators should review documents that show the organizational structure and the chain of command. Investigator should know the mission and function of the organization before interviewing its members. This will help place the information provided by witnesses in context. Similarly, investigators should review individual biographies (most common with senior officials) and personnel records to help develop pertinent questions for each witness.

5.3 Rights and Obligations of Witnesses

5.3.1 A Witness's Protection against Self-Incrimination. DoD OIG witnesses have both rights and obligations depending on their status (civilian or military) and other factors discussed below. Overall, employees have a duty to cooperate with a DoD OIG investigation under the IG Act and DoDD 5106.01. However, all employees have the constitutional right against self-incrimination. If a witness refuses to be interviewed invoking the right against self-incrimination, the investigator should terminate the interview immediately.

5.3.2 Article 31b Warnings (Service Members). Article 31b of the UCMJ requires that whenever a military member whom the interviewer suspects may have committed an offense under the UCMJ is questioned, the member must be advised of the nature of the offense, his or her right to remain silent, and that any statement made may be used against the member. This applies whether or not the member being questioned is in custody or has voluntarily agreed to speak.

5.3.3 Garrity Warnings (Civilians). In 1967, the Supreme Court held that if Federal employees are compelled to answer questions under the threat of losing their Government employment, then the Government may not use the employees' statements or any evidence derived from those statements in any criminal prosecution (Garrity v. New Jersey, 385 U.S. 493 [1967]).

The Attorney General issued guidance and a model Garrity warning to be used by IG investigators in certain situations when interviewing current Federal Government employees, who are either witnesses or subjects of the investigation. Garrity warnings are only given when it's foreseeable that the information sought from the employee may be used to criminally prosecute the employee. However, Inspectors General have discretion in determining the specific circumstances under which a Garrity warning should be given.

Therefore, if investigators are planning to interview a Federal Government employee, as a witness or a subject, on matters that may include potential criminal violations, they should consult with their supervisor and with the OGC on whether to issue a Garrity warning at the start of the interview.

5.3.4 Kalkines Warnings (Civilians). If a Federal employee refuses to cooperate by claiming the Fifth Amendment right against self-incrimination, terminate the interview immediately. The investigator should then consult with an attorney from the OGC and DCIS to determine if a "Kalkines warning" should be issued. A Kalkines warning can only be issued following the receipt of a declination of prosecution in the matter from the U.S. Attorney's Office.

In a Kalkines warning, the witness's supervisor (not a representative of the OIG) informs the witness that the witness' statements to investigators will not be used as evidence against the witness in a criminal prosecution. The witness is also informed that he or she may no longer claim the Fifth Amendment protection against self-incrimination. The witness is told that receipt of a Kalkines warning results in a duty to respond to DoD IG questions. Finally, the witness is informed that the information provided may be used against the witness in agency administrative proceedings and, if agency regulations so state, the witness may be fired from his or her Federal job for continued failure to cooperate.

5.3.5 Union Representation (Weingarten Rights). An employee in a bargaining unit represented by a union may refuse to submit to an investigatory interview without union representation being present, if the employee has a reasonable belief that the examination may result in disciplinary action. It is the employee's right—not a union prerogative. The union representative may not demand to be present against a witness's or employee's objections. If an employee in a bargaining unit represented by a union requests union representation, the investigator must grant the request, discontinue the interview, or offer the employee the choice of continuing the interview without representation. If the union representative is not immediately available, the investigator must reschedule the interview to permit the employee a reasonable amount of time to get a union representative.

5.3.6 Legal Representation. Investigators should allow witnesses to have their attorney present during interviews, provided certain conditions are met. It should be a private attorney or military-appointed defense attorney. DoD Agency attorneys or military attorneys assigned as staff judge advocates should not represent the interests of an individual during a DoD IG interview since their responsibility is to represent the Government's interests.

Should a subject request to have an attorney present, before the interview, the investigator should request that the subject provide written confirmation that the attorney has been retained in a private capacity for civilian employees or has been appointed by appropriate authority in the Service Judge Advocate General's office for Service members. This is significant as the DoD IG does not allow DoD organization or command attorneys to attend interviews for the purpose of representing the interests of individual employees. Should the need arise to interview the DoD organization or command attorney for the investigation, do so separately to ensure the integrity of the investigation.

Following the read-in, the investigator should clarify the role of the attorney on the recording.

5.3.7 Minor's Right to Have Parents Present. If a witness is under the age of 18, investigators should arrange for a parent to be present during the interview.

5.3.8 Right to an Interpreter. If a witness has a better grasp of matters in his or her native language, the investigator should consider arranging for an interpreter to be present during the interview. The investigator is responsible for obtaining the interpreter. Do not rely on the witness to obtain one.

5.3.9 Obligations or Duties of Individuals Involved in IG Investigations

5.3.9.1 Service members and Federal Employees. Service members and Federal employees must cooperate in IG investigations and inquiries. Commanders and supervisors may order those who refuse to cooperate to do so.

5.3.9.2 Non-Federal Civilians. Non-Federal civilians cannot be compelled to cooperate with an IG conducting an investigation or inquiry absent the issuance of an IG testimonial subpoena.

5.3.9.3 DoD Contractor Employees. DoD contractor personnel are considered to be non-Federal civilians; however, they may have an obligation to cooperate with IG investigations and investigative inquiries if the contract employing them with the Government requires them to cooperate. In these situations, contact the contracting officer and work through them to obtain witness cooperation.

5.4 Witness Confidentiality

Section 7(b) of the IG Act states that the Inspector General must not, after receipt of a complaint or information from an employee, disclose the identity of an employee without the employee's consent, unless the Inspector General determines that such disclosure is unavoidable in the course of the investigation. Investigators should inform witnesses that the DoD IG is committed to protecting their confidentiality to the maximum extent possible within the law; however, there may be some circumstances when the IG determines that releasing their identity or testimony is necessary or unavoidable. For example, in whistleblower reprisal cases, it will be necessary to disclose the name of the whistleblower who is claiming reprisal to conduct the investigation.

5.5 Authority to Administer Oaths

Under the IG Act, each Inspector General is authorized to administer to or take from any person an oath, affirmation, or affidavit, whenever necessary in the performance of the duties under the Act. See Inspector General Act, Section 6(a) (5)).

5.6 Sworn Recorded Testimony

5.6.1 Purpose of Recording. It is ODIG AI policy to obtain sworn recorded testimony from all complainants, subjects, and primary witnesses who are interviewed. Interviews are recorded to ensure a complete and accurate record of the witness's testimony and improve the accuracy and quality of the ROI.

5.6.2 Witness Acknowledgement. It is ODIG AI policy that all witnesses will acknowledge on the record that they are aware the interview is being recorded. Before the start of an interview, the investigator should explain to the witness that ODIG AI policy is to record interviews. The investigator should explain that the purpose of recording is to ensure accuracy and, if requested, the witness may be provided a copy of the transcript after the investigation is complete. When the recorded interview begins, the investigator should ask the witness to verbally acknowledge that the interview is being recorded.

5.6.3 Telephone Interviews. Telephone interviews may also be recorded. If the telephone interview is to be recorded, it is imperative to have the witness acknowledge on the record that he or she knows the interview is being recorded.

5.6.4 Recording by Witnesses. It is ODIG AI policy that witnesses are not authorized to record their interviews. The term witness in this situation applies to complainants, witnesses, and subject or subjects, and their attorneys. This is intended to preserve the integrity of the investigation, and to protect the confidentiality, rights, and privacy of all individuals involved.

5.6.5 Standard Read-In and Read-Out Process. Investigators must follow the standard pre-recording read-in and read-out process. This is to ensure that all witnesses are treated equally and receive the proper notifications of authorities; due process; general rights; and warnings, as appropriate, such as Garrity and Kalkines warnings.

5.6.5.1 Pre-Recording Discussion. Investigators will address the following before turning on the recorder.

- Introduce the investigator and display credentials.
- Advise the witness that this is an administrative (not criminal) investigation.
- Briefly state the purpose of the interview and explain why it is necessary to interview the witness.
- Inform the witness that the interview will be conducted under oath and that it will be recorded; remind the witness that even when the recorders are off, nothing is off the record.

- Review and provide the witness with a copy of the Privacy Act Notification if needed.

- Unless special recording devices and arrangements have been made in advance, remind the witness that nothing classified may be discussed while recording.

5.6.5.2 Read-In. The standard read-in will include the following.

- State the date, time, and location of the interview.

- Introduce the investigators.

- Identify the allegations.

- State that the employee is a witness or subject.

- Rights Advisements – as applicable.

- Administer the oath;

- Confirm the interview will be recorded.

- Confirm the Privacy Act was provided.

- Witness states his or her name and title.

5.6.5.3 Read-Out. The standard read-out will include the following.

- Ask if the witness wishes to provide any additional information.

- Ask if the witness has any questions.

- Caution the witness not to discuss the testimony with anyone, except for his or her attorney, an Inspector General, or a Member of Congress.

5.6.6 Recording Interviews

5.6.6.1 Make a Good Record. It is important that the transcript of an interview is a clear and accurate record of the testimony by the witness. Following the steps below will help enhance the quality of the recording.

1. Ask the witness to speak loudly and clearly at the start of the interview and at any time during the interview if the witness starts to mumble or speak in a soft or lowered voice.

2. Ask the witness to explain any acronyms and spell out any questionable words or names.

3. If the witness makes nonverbal gestures such as head nods or hand movements, direct the witness to provide audible responses.

4. Identify verbally any documents that are introduced during the interview. Refer to them by name, date, and page or paragraph number.

5.6.6.2 Handling "Off-the-Record" Statements. Sometimes witnesses may desire to make statements "off-the-record" during the course of an interview and request that the recorder be turned off. Caution the witness that stopping the recording does not constitute going "off the record" and that anything said may be used as part of the investigation. If the investigator turns off the recorder to hear what the witness has to say, then the investigator, upon hearing the information, should determine if it is relevant to the investigation and go over the information with the witness with the recorder turned on. The following two techniques may be effective in this situation.

- Ask specific questions of the witness to elicit the relevant information.

- Summarize "off-the-record" comments made by the witness and ask the witness to verify them. Note: As a less preferable alternative, you may document the "off-the- record" discussion in a memorandum for record.

5.6.6.2.1 Transcription Request Form. Investigators should exercise care and attention to detail in completing a transcription request form. They should ensure all names, locations, and acronyms are spelled out, and identify anything a person outside the DoD would not recognize.

5.6.6.2.2 Validating Transcripts. Investigators should validate transcripts by listening to the audio recording and comparing it to the transcript. They should do this for the key statements cited in the ROI in support of the report's conclusions, and also for inaudible audio segments that appear in the transcript

5.7 Interview Techniques

A variety of interview techniques may be employed, depending on the nature of the investigation and the circumstances of a particular situation. Interviews commonly have four phases: background, free narrative, direct questioning, and cross-examination.

5.7.1 Background Phase. During the background phase, the investigator should ask questions to establish the biographical information of individuals and organizations relevant for that particular witness. This will include questions relating to the witness's title or position,length of time in that position, responsibilities, and organizational and chain-of-command relationships.

5.7.2 Free Narrative/Indirect Questioning Phase. During the free narrative/indirect questioning phase, the investigator should ask open-ended questions, asking the witness to talk about knowledge of the events or actions under investigation in his or her own words without interruption. This may also be a good time to ask the witness to talk about processes that relate to the matters under investigation. This gives the witness the opportunity to provide his or her unique memory and perspective of events, resulting in the investigator developing a more complete picture of events and obtaining information that was previously unknown.

5.7.3 Direct Questioning Phase. During the direct questioning phase, the investigator should ask questions about the details of the events with a specific focus on the allegations of misconduct, the elements of proof, and individual accountability. This set of questions will typically include questions like "did you or did they" and "why did you or why did they?" During this phase, it is important to pin down the subject, require the subject to answer the questions, and not let the subject evade or avoid the questions.

5.7.4 Cross-Examination Phase. During the cross-examination phase, the investigator should address inconsistencies in the witness's testimony, contradictions within the testimony, or conflicts between the witness's testimony and other witnesses' testimony. This is also the phase in which the investigator should put the subject or witness on notice if the investigator believes the witness is not being honest or truthful in his or her testimony. This is a good time to remind the witness of the responsibility to provide truthful testimony. This is a critical phase of the interview and it is important for the investigator to not leave critical questions unasked or conflicts unaddressed.

5.8 Privileged Information

Witnesses may claim a "privilege" that prevents them from cooperating with the investigator. The following claims are most commonly encountered and should not be considered as an inclusive list. If you have any questions regarding issues of privilege, consult with your supervisor or the OGC.

5.8.1 Promotion Boards. Board members, recorders, and support personnel are sworn to secrecy. If you must interview these individuals regarding board proceedings, obtain a memorandum from the Military Department Secretary releasing them from their oaths.

5.8.2 Attorney-Client. A client has a privilege to refuse to disclose, and to prevent any other person from disclosing, confidential communications made to facilitate professional legal services to the client.

5.8.3 Husband-Wife. A person has a privilege to refuse to testify against his or her spouse.

5.8.4 Priest-Penitent. A person has a privilege to refuse to disclose, and to prevent another from disclosing, a confidential communication by the person to a clergyman or a clergyman's assistant, if such communication is made either as a formal act of religion or as a matter of conscience.

5.8.5 Doctor-Patient. Many witnesses (and medical professionals) believe that communications between a patient and a doctor are protected by privilege similar to the attorney-client privilege described above. However, under Federal law, such privilege generally does not exist except under certain circumstances between a psychotherapist and his or her patient. Furthermore, there is no privilege regarding the medical treatment of military personnel, military family members, or civilian employees by Government physicians. For example, a military doctor must testify regarding his or her treatment of a Service member. Additionally, ISO and WRI investigators may also gain access to treatment records maintained by Government medical facilities.

CHAPTER 6—FINAL REPORTS

6.1 Introduction

The third qualitative standard of the CIGIE "Quality Standards for Investigations," "Reporting," requires that "reports (oral and written) thoroughly address all relevant aspects of the investigation and be accurate, clear, complete, concise, logically organized, timely, and objective." ODIG AI reports should create a formal record of the allegations that initiated the investigation, the scope of the investigative effort, the issues addressed by the investigation, the evidence collected, and the conclusions reached as to whether a violation or misconduct occurred. All ODIG AI reports should reflect the guidelines set forth below.

6.2 Professional Standards Guidelines

6.2.1 Accurate. One of the most important professional quality standards for investigative reports is that they must be accurate. DoD OIG reports can have profound effects on the careers of DoD employees and on the public's trust and confidence in DoD officials and the IG organization as a whole. Investigators must exercise due professional care in accurately reporting the findings of their investigations. Investigators must treat this responsibility seriously and must pay close attention to details in reporting factual information. Investigators should not make errors identifying people, places, dates, events, activities, or other basic factual information, nor should they make any errors presenting witness testimony. Investigators should exercise care presenting witness testimony in the report to ensure that it is accurate, and that it has not been inaccurately paraphrased or characterized. Errors in basic facts or in testimony have the potential to undermine the overall credibility of the report, the investigation, and the IG organization. To avoid errors in writing, investigators must write from source documents, not from their memory.

6.2.2 Documentation. The facts presented by investigators in reports must be fully supported by documentation. The documentation must be easily traceable by reference in a comment box that contains a hyperlink to the document in D-CATSe and identifies the location within the document of the reported facts. Source documents for facts presented in the report should be maintained in the Report of References folder in D-CATSe. Source documents include official records (such as personnel records, travel records, contract records, and timesheets), testimonial evidence (such as pages from transcripts, reports of interviews, and e-mails), and other evidence collected during the investigation.

6.2.3 Clear. Investigators should use the plain language style of writing and use active voice to give the reader a clear understanding of the basic facts of the case and the logic used to arrive at the conclusions. Reports should be well-organized and structured around the issues and the elements needed to prove or disprove misconduct. They should also clearly communicate the analysis of the evidence, including the credibility of the witnesses, how the evidence was weighed, and how conflicting evidence was resolved.

6.2.4 Thorough. Reports should contain enough information to allow an uninformed reader to understand the allegations that were raised, what the investigation found, and the basis for the DoD IG conclusions. DoD OIG reports should demonstrate to the reader that the allegations were treated seriously and the investigation was a diligent effort to ascertain the facts. Reports that

lack sufficient information may raise doubt in the reader's mind about the credibility of the investigation and the DoD OIG.

6.2.5 Complete. Reports should document a complete record of the issues addressed by the investigation, the relevant supporting evidence, and investigative activities, and adequately discuss the analysis of the evidence, thereby answering the reader's anticipated questions on important aspects of the investigation. In cases in which one or more of the allegations are not investigated, they should be noted in the report to avoid lingering questions regarding the disposition of those allegations.

6.2.6 Standards. Reports will contain the standards applicable to the matters under investigation. Standards should be listed precisely, carefully citing the complete title, sections, dates, and relevant language verbatim. Investigators will not paraphrase regulations.

6.2.7 Concise. Reports should be concise and to the point, presenting only the information that is relevant and essential to resolve the issues. Reports should be direct and focused only on the relevant issues—not a regurgitation of all the information developed during the investigation. Sentences or paragraphs that attempt to convey multiple thoughts or that stray from the issue may confuse the reader and should be avoided. Long, rambling reports lose the reader and only succeed in obscuring critical information. Reports will reflect the guidelines of the Plain Writing Act of 2010, which requires Federal agencies to write clear Government communication that the public can understand. The Federal Plain Language Guidelines include using active voice, short sentences, short paragraphs, useful headings, and tables. Following these guidelines will help make reports more clear, concise, and readable.

6.2.8 Objectivity. Reports should be fair, impartial, and free of bias. They should present both sides of the story: the evidence in support of the allegations and the evidence casting doubt on the allegations. They should contain information presented by the subjects in their defense, including information that is non-incriminating, mitigating, or in dispute. Investigators' personal opinions are not to be included in DoD OIG reports.

6.3 Report of Investigation

ODIG AI employs the write-as-you-go process to produce reports in a more timely and efficient manner. Investigators will start the writing process upon the initiation of fieldwork. Facts should be entered in the draft report upon discovery, and will be hyperlinked to source documents immediately upon entry. Investigators, supervisors, and OGC attorneys will review the draft at roundtable discussions throughout the fieldwork phase, resulting in a substantially written draft report upon the completion of fieldwork. The drafts should not include conclusions until sufficient evidence has been gathered to form a conclusion based on the preponderance of clear and convincing standards.

Investigators will use the standard templates for writing reports of investigation. Except in summary reports, the following sections should appear in each report.

6.3.1 Executive Summary or Introduction and Summary. The Executive Summary or Introduction and Summary should be a one- to two-page, stand-alone section of the report designed to give the reader the most important information contained in the report, in the most concise

manner. The main elements of the Executive Summary and the Introduction and Summary are described below.

6.3.1.1 Introductory Paragraph. This investigation was conducted in response to allegations that (name of senior official) misused Government resources relating to official travel OR that (name of whistleblower) suffered reprisal for reporting wrongdoing.

6.3.1.2 Conclusion Paragraph. We conclude that (name of senior official) misused Government resources OR that (name of subject in whistleblower reprisal) issued an adverse officer evaluation report in reprisal for (complainant's) protected communication or disclosure.

6.3.1.3 Recommendation Paragraph. We recommend that appropriate corrective action be taken regarding the senior official or the subject. We also recommend that the senior official reimburse the Government OR that appropriate remedial action be taken to correct the personnel action taken in reprisal against the whistleblower.

6.3.2 Background. This section gives the reader information about the organizations, command relationships, and key individuals involved in the investigation. It may also provide a chronology or synopsis of key events related to the matters under investigation. Chronologies in this section should be brief and are not intended to be detailed narratives of the facts of the case that are presented in the Findings and Analysis section of the report.

6.3.3 Scope. This section describes the scope of the investigation in summary terms including information describing the timeframe addressed by the investigation, the documents that were reviewed, the key witnesses who were interviewed, and any other special investigative techniques that were employed such as the use of subpoenas. This section also addresses allegations that were not investigated because they were not within the scope of the investigation.

6.3.4 Findings and Analysis. This section presents the main findings of the report in a format comprised of standards, facts, discussion, and conclusions, organized under each of the issues and allegations addressed by the report. Note: In WRI reports, the standards are presented in a separate section, Legal Framework which precedes the Findings and Analysis section.

6.3.5 Standards/Statutory Authority. Investigators should refer to report template instructions posted on the AI SharePoint site for additional guidance on the input of statutory or regulatory language in the report. For ISO reports, investigators will use the report template and refer to the standards library for the applicable statutes and regulations. For WRI reports, investigators will use the template created for the statute that applies to their investigation. This language is locked down and should not vary from report to report. Over time, investigators may find standards sections for their investigations in the electronic library on the shared drive or SharePoint site.

6.3.6 Facts. This section presents the who, what, when, where, why, and how, relating to the issues and allegations under investigation. Investigators should present the facts, including names, dates, organizations, and locations, with testimony that is clearly attributed to a source. Investigators may use the term "witness" or use an employee's title when presenting testimony, where appropriate, to protect witness confidentiality or personal privacy information.

The facts should be presented in a manner that addresses the elements of proof needed to substantiate or not substantiate the applicable standard or statutory authority. It may also be

helpful for investigators to use subheadings in this section to help with the organization and readability of complex matters.

The source document supporting statements of facts and testimony must be cited when writing the report and accurately hyperlinked to the appropriate documentation.

6.3.6.1 Citing Sources. Citing source documents is critical in meeting professional standards and in performing the quality review process. All facts referenced in a report must contain a hyperlink to a cited source; this includes the original complaint, referenced standards that are not foundational to the AI mission, footnoted information, quotes, and information appearing in tables. Investigators must use the track changes and comment boxes containing hyperlinks to reference the source document and identify the location of the reported information; for example, (hyperlink) Smith Testimony, page 12: 2-20; (hyperlink) Email dated 01-01-2022 ,page 1 paragraph 3; or (hyperlink) Personnel Document, page 2, table 1, row 4.

6.3.7 Discussion. In this section investigators explain how they arrived at the conclusions. The language should plainly state that we have analyzed the evidence using the applicable standard of proof; for example, "preponderance of evidence" or "clear and convincing."

The Code of Federal Regulations (CFR) defines the standards:

- "Preponderance" of the evidence is that degree of relevant evidence that a reasonable person, considering the record as a whole, would accept as sufficient to find that a contested fact is more likely to be true than untrue. See title 5 CFR section 1201.56 (c)(2).

- "Clear and convincing" evidence is that measure or degree of proof that produces in the mind of the trier of fact a firm belief as to the allegations sought to be established. It is a higher standard than preponderance of the evidence but a lower standard than beyond a reasonable doubt. See title 5 CFR section 1209.4(d).

Black's Law Dictionary defines the standards as follows.

- Preponderance of the evidence is evidence that is of greater weight or more convincing than the evidence offered in opposition to it; that is, evidence that, as a whole, shows that the fact sought to be proved is more probable than not. It is the greater weight of evidence, or evidence that is more credible and convincing to the mind.

- Clear and convincing evidence is the proof that results in a reasonable certainty of the truth of the ultimate fact in controversy. Clear and convincing proof will be shown where the truth of the facts asserted is highly probable.

The Discussion section must be clear and persuasive. Investigators should start the discussion section by stating the conclusion in the first sentence, and then follow with information that walks the reader through how the evidence supports the conclusion.

Investigators should follow the elements of the applicable regulations and explain how the facts apply to those elements. They should not merely restate all of the facts in the Discussion section. On the other hand, they should not assume that anything, particularly their logic, is

obvious. They need to be explicit in pointing out the specific facts that carried the most weight in reaching the conclusion.

It is especially important for investigators to deal with the arguments put forward by the subject of the investigation, and explain how they were considered in reaching the conclusions. Note: If a Preliminary Conclusion Letter (PCL) was issued, investigators should incorporate the subject's responses and arguments in the final report. Also, investigators should address any additional fieldwork that was conducted subsequent to the PCL response, any new information discovered by the additional investigation, and how the new information impacted the tentative conclusions.

6.3.8 Conclusions. This section sets forth the conclusions for each allegation addressed in the Findings and Analysis section of the report. The conclusion statement for each allegation should be one sentence that identifies the misconduct and the regulation that was violated, as shown in the following examples.

- We conclude that the senior official misused Government resources in violation of (cite the regulation).

- We conclude that subject (use the name of the individual) issued (put complainant's name) an unfavorable Noncommissioned Officer Evaluation Report (NCOER) in reprisal for his or her protected communications, in violation of (cite the statute or regulation).

When there are multiple conclusions, the section should start with the following statement.

We conclude that:

- The senior official misused Government resources in violation of (cite the regulation).

- The subject (use the name of the individual) issued (put complainant's name) an unfavorable NCOER in reprisal for his or her protected communications, in violation of (cite the statute or regulation).

6.3.9 Other Matters. The Other Matters section may be used to report systemic issues identified during the course of the investigation. Examples of topics for the area include weaknesses in policies or procedures, areas of mismanagement, command climate, or morale issues.

6.3.10 Recommendations. This section makes recommendations for corrective actions.

6.3.10.1. In cases where misconduct is substantiated, investigators should recommend appropriate action. We do not recommend disciplinary action. For example:

- We recommend that the Secretary of the (Military Department) take appropriate action with respect to the (senior official/subject).

6.3.10.2. In cases where relief for the complainant is appropriate, investigators should recommend remedial action. For example:

- We recommend that the Secretary of the (Military Department) take remedial action with respect to (complainant's name) unfavorable NCOER.

6.3.10.3. In cases where reimbursement to the Government is appropriate, investigators should recommend reimbursement. For example:

- We recommend that the Secretary of the (Military Department) direct the General reimburse the Government for his or her misuse of Government resources for unofficial purposes.

6.3.10.4. In cases where systemic issues are identified, investigators should recommend specific corrective action. For example:

- We recommend that the Secretary of the (Military Department) direct (title of appropriate management official) (establish/strengthen/clarify) policies and procedures governing official travel.

6.3.10.5. In cases where no corrective action is required, investigators should state that we make no recommendations. For example:

- We make no recommendations in this matter.

6.3.11 Footnotes. Footnotes should be used sparingly to cite additional explanatory language in support of statements in the body of the report. This allows the reader to focus on the facts without interruption, if they so choose. Footnotes should not be used to cite sources. That is accomplished through hyperlinks placed in comment boxes.

6.4 ROI Review Process

6.4.1 Review Process. All ODIG AI final reports will undergo a quality review process in keeping with Inspector General Instruction 7600.01, "Quality Standards for DoD Office of Inspector General Oversight Work," January 2, 2024 (Incorporating Administrative Change, June 16, 2024). The quality review process ensures that final reports meet the professional standards for quality and that they are thorough, factually accurate, legally sufficient, and professionally prepared. The review process includes a peer review, a supervisor review, an editor review, an independent quality assurance review, a legal review, and a DDIR/DIR review.

This is a collective process that requires each member to accomplish their role with due diligence to produce reports that reflect the highest standards for quality and professionalism. All of those involved in producing reports must be mindful that ROIs are the product of the DoD OIG. By CIGIE standards, investigators have a responsibility to be impartial, to remain objective, and to be receptive to evidence that is non-incriminating as well as incriminating. Moreover, investigators should not allow conjecture, unsubstantiated opinion, bias, or personal observations or conclusions to affect their work.

6.4.2 Review Edits. At each step in the review process, read the edits and make sure they do not inadvertently change the meaning of a sentence or, especially, alter a fact.

6.4.3 Peer Discussion and Review. Investigators should have a peer review of their draft report. Generally, this is the first chance for another individual to put a fresh set of eyes on the draft report to identify areas where facts are missing or where the facts as presented do not logically flow to the conclusions. Additionally, it is helpful to have an investigator who has little or no knowledge of the case review the draft. This investigator can provide an independent "sanity check" of the effort.

As a general rule, the more experienced the reviewing investigator, the greater the "value added" to the report. If another investigator assisted during the fieldwork, particularly during the interviews, that person should also review the draft report. This not only provides feedback on the report format, language, and presentation, but also provides a critical review of the analysis, conclusions, and recommendations.

6.4.4 Supervisor Review

6.4.4.1 Following the peer review, the investigator will edit the report and inform the SI that it is ready for the first supervisor review.

6.4.4.2 The SI will review the report by providing edits and comments using track changes, and by returning the draft report for revision as appropriate. The SI review will include a review of the supporting evidence by checking each hyperlink to source documents to ensure that the factual statements in the report are accurate. The investigator will revise the draft report as directed by the SI. The SI will then ensure that the directed changes were made in the report.

6.4.4.3 Deputy Director or Director Review (DDIR/DIR). Once the SI is satisfied with the draft report, he or she will inform the DDIR/DIR, who will then review the report, make edits and comments in track changes, and return it for the investigator to make changes to the draft report as directed.

6.4.5 Editor / Quality Assurance

6.4.5.1. Editor Review. The editor will proofread the report to identify errors in grammar, syntax, spelling, and typing, and will ensure the proper template is used. The editor will verify that acronyms, names, and military ranks are used appropriately. The editor will verify that all standards and statutes are cited correctly. The editor will check for compliance with the "Style Manual and Reference Tool (SMART)," the "Government Publishing Office Style Manual," and Federal plain language guidelines. The editor will verify that the report is compliant with 508 guidelines. The editor will check for correct line and page endings. The editor will review the structure, content, and organization of the report to ensure a clear focus and alignment with the target audience. The editor will return the ROI to the investigator for review.

6.4.5.2. Quality Assurance Review. As part of the ODIG AI Quality Assurance Program, the ODIG AI Program Analyst for Quality Assurance will perform an independent review of the draft ROI. The program analyst is organizationally independent of the ISO and WRI Directorates and has not been involved in conducting the investigation or the report writing process. This independent review is performed to ensure compliance with CIGIE standards for accuracy, documentation, and clarity. The program analyst reviews evidence, source documents,

and witness testimony supporting factual statements in reports to ensure the factual accuracy and supportability of the report. The program analyst will identify potential inconsistencies or errors and return the report to the investigative team for updates deemed warranted. The program analyst will complete the Quality Assurance Review Checklist and save it to D-CATSe.

6.4.6 Office of General Counsel Review. Once the Editor and Quality Assurance reviews are complete, the report will be sent to the OGC for a review. The OGC-assigned attorney will review the report for legal sufficiency, which includes ensuring the conclusions are supported by the evidence. If required, the investigative team and the OGC attorney will hold a roundtable discussion to efficiently and effectively resolve any questions or concerns. Candid and clear communication will reduce the number of iterations in the draft review process and move the investigation more rapidly toward completion. After the investigator revises the draft report, it must be submitted to the OGC for a review and concurrence that it is legally sufficient.

6.4.7 DIG AI Review. Once a report has been approved by the director, edited, found to comply with CIGIE standards by the QA reviewer, and found legally sufficient by the OGC, it is ready for review by the DIG AI. The DIG AI will review the report and either return the report to the Directorate to make edits as directed or instruct the Directorate to forward the report to the IG Front Office.

6.5 Report Approval

6.5.1. Once the report has been cleared by OGC for legal sufficiency and approved by the DIG AI as the Final Draft, the report is ready to be submitted to the IG Front Office for approval.

- The Final Draft report is uploaded to a subpage located on AI's main SharePoint labeled "ISO-Final Draft ROI to IGFO" and "WRI-Final Draft ROI to IGFO." Only final drafts ready for IG Front Office review should be uploaded here. It is in this location that final edits required by the IG Front Office will be addressed.

- The Final Draft ROI is shared with the IG Front Office by means of the IG FO Reviews tool.

Once in the IG front office, the report will be reviewed and may be edited by the executive staff, the PDIG, or the IG. If the PDIG or the IG has questions, the report and the related correspondence may be returned to the DIG AI, director, or directly to the investigator for additional action.

6.5.2. Returned Reports. If substantive modification to the report is required, investigators should ensure the revisions are coordinated with the DIG AI and the OGC. Investigators should pay particular attention to continuity in tracked changes. Changes made to conclusions and recommendations may require alteration of wording in Findings and Analysis and in the Executive Summary/Introduction and Summary. Alterations to the Executive Summary or Introduction and Summary section must be carried forward into closure memorandums and letters.

6.5.3. Distribution. Once the IG approves the report, the IG or appropriate ODIG AI official will sign any applicable closure memorandums and letters. At this point the report is ready for distribution. Procedures for distribution of documents, potential release of information, and disposition of files are discussed in Chapter 7, Case Closure.

6.6 Preliminary Conclusion Letters

In investigations in which misconduct is substantiated, the ODIG AI will provide the subject a PCL and an opportunity to comment on the preliminary conclusion before issuing a report.

The PCL package comprises a letter addressed to the subject of the investigation (or his or her attorney) and a copy of the draft ROI, which has been redacted for source protection. The PCL will include the following statement: "Because information in this letter and the draft ROI are exempt from public release under the Freedom of Information Act, they are designated Controlled Unclassified Information and may not be copied or further released."

PCLs are either hand-carried, or delivered by certified mail, express mail, or e-mail. Subjects are generally given 2 weeks from the date of the letter to respond. Comments made by the subject or subjects will be considered, and additional investigation will be conducted, if necessary. The subject's comments will be incorporated into the final report, along with the ODIG AI written analysis of the impact of the subject's comments on the report's findings and conclusions.

CHAPTER 7—CASE CLOSURE

7.1 Introduction

The third general standard of the CIGIE, "Due Professional Care," requires that the investigative report findings and accomplishments are supported by adequate documentation. To ensure compliance with these standards, it is important for investigators to perform all of the tasks critical to the case closure process, and to fully document the outcome of the investigation.

7.2 Case Closure Process

Once the final report is approved, investigators should promptly accomplish case closure procedures.

Steps in the Case Closure Process:

1. Prepare the closure correspondence.
2. Following the staffing process:
    a. For Director Signature
    b. For DIG AI Signature
    c. For IG signature or Director, OLAC signature
3. Enter the data in D-CATSe.
4. Prepare the case file.

7.3 Closure Correspondence

Investigators will prepare closure correspondence and staffing packages as soon as possible following the determination of legal sufficiency of the final ROI by the OGC and the approval of management. Investigators bear the primary responsibility for ensuring that closure correspondence and staff packages are complete, accurate, and properly assembled using the standardized templates and in accordance with the guidance set forth in the Correspondence Guide. Failure to pay attention to the quality of the closure documents will result in additional work by those involved in the staffing process and unnecessary delays in the closure of the case. Products are a reflection on OIG credibility and professionalism as a whole. When preparing closure letters to the subjects and complainants, be sensitive to the privacy rights of individuals involved in the investigation.

All staffing packages will be assembled as directed by the "DoD Manual for Written Material: Correspondence Management" in hard copy, as required; or electronically in D-CATSe, as described in the following subsections.

7.3.1 Internal DoD Correspondence. Investigators must use memorandums when electronically transmitting the results of investigations to management officials and Inspectors General within the DoD.

7.3.1.1 Internal DoD Correspondence for Reprisal Cases. The memorandum will be prepared for the DIR, WRI signature, and the staffing package must include:

- e-mail forwarding the package to the DIR, WRI with hyperlinks to the appropriate closure correspondence;
- a memorandum transmitting the final ROI to the appropriate officials, including a brief summary of the investigation findings; and
- the ROI.

Templates for ODIG AI correspondence can be found in AI SharePoint.

- For WRI: WRI Correspondence Hub
- For ISO: ISO Toolkit/ISO Templates

7.3.1.2 Internal DoD Correspondence for Senior Official Cases. The memorandum will be prepared for the DIG AI signature except in special high-interest cases in which it should be prepared for the Inspector General to sign when addressed to the Secretary or Deputy Secretary of Defense or Military Department Secretaries. The staffing package must include:

- an e-mail to DIG AI with hyperlinks to the ROI and case closure documents;
- an action memorandum to the IG in special high-interest cases or substantiated cases explaining why their signature is being requested; the memo should provide a brief background and summary of the investigation findings;
- a memorandum to the DoD management official transmitting the final ROI, which will provide a brief summary of the investigation findings;
- the ROI (redacted and unredacted;
- the PCL response as applicable; and
- a letter or letters to the subject or the subject's attorney.

Templates for ODIG AI correspondence can be found in AI SharePoint.

- For WRI: WRI Correspondence Hub
- For ISO: ISO Toolkit/ISO Templates

7.3.2 External Correspondence. Investigators must use letters when reporting or transmitting the results of investigations to complainants, subjects, and Members of Congress.

7.3.2.1 External Correspondence for Reprisal Cases. The letter to the complainant will be prepared for the DIR, WRI, and the electronic staffing package in D-CATSe must include:

- a letter to the complainant transmitting the redacted ROI; this letter provides a brief summary of the investigation findings;
- the redacted ROI; and
- letters to appropriate officials.

Templates for ODIG AI correspondence can be found in AI SharePoint:

- For WRI: WRI Correspondence Hub
- For ISO: ISO Toolkit/ISO Templates

7.3.2.2 External Correspondence for Senior Official Cases. The letter to the subject of the investigation will be prepared for the DIG AI signature, and the electronic staffing package in D-CATSe must include:

- an e-mail to the DIG AI with hyperlinks to the ROI and closure correspondence; and
- the letter to the subject of the investigation informing the subject that the investigation has been completed, and providing a brief summary of the conclusions of the investigation. In substantiated cases, the subject is also informed that the appropriate management official has been provided a copy of the ROI for appropriate action.

Templates for ODIG AI correspondence can be found in AI SharePoint.

- For WRI: WRI Correspondence Hub
- For ISO: ISO Toolkit/ISO Templates

7.4 Congressional Inquiries

7.4.1. Correspondence. The letter to the Member of Congress will be prepared for the signature of the Director, OLAC, and the electronic staffing package in D-CATSe must include:

- an action memorandum to the Director, OLAC providing a summary of the investigation findings;
- TAB A: A letter to the Member(s) of Congress providing a summary of the findings of the investigation consistent with the Privacy Act restrictions on release of information (see the guidance below);
- TAB B: A copy of the incoming Congressional;

- TAB C: Previous correspondence (interim responses sent previously); and
- TAB D or the last TAB is always reserved for coordination.

Templates for ODIG AI correspondence can be found in AI SharePoint.

- For WRI: WRI Correspondence Hub
- For ISO: ISO Toolkit/ISO Templates

7.4.2. Types of Congressional Requests. A Member of Congress may write in one of three capacities: individual, on behalf of a constituent, or on behalf of a committee.

7.4.2.1. If a Member of Congress writes in his individual capacity and not on behalf of a constituent, the letter may contain only information that is releasable to the public. The findings will be provided in an Executive Summary format and will not contain information that would not be released under the Freedom of Information Act. The letter and enclosure will not be marked CUI.

7.4.2.2. If the Member of Congress writes on behalf of a constituent, the letter to the Member will contain information that would be released to the constituent directly. The letter and any enclosure will be marked CUI and include the following paragraph.

> Because information in this letter may be exempt from public release under the Freedom of Information Act (FOIA), the letter is designated "CONTROLLED UNCLASSIFIED INFORMATION." This letter may be released to [insert name of constituent], but other requests for this letter should be referred to the DoD Office of Inspector General, FOIA Requestor Service Center, 4800 Mark Center Drive, Suite 17F18, Alexandria, VA 22350-1500.

7.4.2.3. If the Member has written the DoD IG in his capacity as a chairman (and in some cases, ranking member) of a congressional committee or subcommittee, the member may be provided an unredacted version of the report. If the report is CUI, the closure letter will, in all likelihood, also contain CUI information. In such cases, the following paragraph will be included in the correspondence to the chairman.

> Because information in this letter and the enclosed report may be exempt from public release under the Freedom of Information Act (FOIA), they are designated "CONTROLLED UNCLASSIFIED INFORMATION." As such, this letter and the enclosed report are provided to you in your role as Chairman (or Ranking Member) of a committee of jurisdiction with respect to the subject matter, are for the exclusive use of your committee, and may not be released to the public. Therefore, we ask that you coordinate any additional users or releases with the DoD Office of Inspector General, FOIA Requester Service Center, 4800 Mark Center Drive, Suite 17F18, Alexandria, VA 22350-1500.

7.5 Information Management

The fourth qualitative standard of the CIGIE "Quality Standards for Investigations," "Managing Investigative Information," requires that investigative data be stored in a manner allowing effective

retrieval, referencing, and analysis, while ensuring the protection of sensitive data (for example personally identifiable information). An effective management information system should allow management to have information to perform its responsibilities, to perform trend analysis, to measure accomplishments, to produce semiannual reports to Congress, and to respond to requests by external customers.

The CIGIE general investigative standard for due professional care requires that investigative report findings and accomplishments must be supported by adequate documentation and maintained in the case file.

The CIGIE qualitative investigative standard for managing investigative information requires that all investigative activity, both non-incriminating and incriminating, should be recorded in an official case file.

It is the investigator's responsibility to ensure that investigative data is current, complete, and accurate, and that case files are well-organized and complete from case initiation through case closure. Maintaining the file during the investigation affords the prompt retrieval and analysis of evidence throughout the course of the investigation. The case should always be maintained in a manner in which another investigator or management official could quickly access the file and obtain an understanding of the case from the key evidence collected to that point in time. Upon case closure, investigators will ensure that all the evidence and other documentation is in the file and in the proper location to have the file ready for potential FOIA requests or other requests for investigation documents. Closed case files should also be ready to withstand scrutiny by an outside peer review or oversight authority.

7.6 Case File Organization

7.6.1. Master File. The master file with documents relating to the investigation are placed in SharePoint through D-CATSe via the Documents link. This allows for quick retrieval of the documents. A description of the documents to be placed at each tab is set forth below.

7.6.1.1. Folder 01 – Complaint & Supplementals. Reserved for the incoming complaint and notification to the Component IGs. In addition, this folder is reserved for any supplemental information to the complaint.

7.6.1.2. Folder 02 – Intake. Reserved for documentation related to the intake process. In addition, this folder is reserved for the DoD IG referral to the component IGs.

7.6.1.3. Folder 03 – Investigative Planning. Reserved for the investigative planning documentation. The investigative planning folder is divided into the following subfolders.

A. Investigative Plan. Reserved for the initial and final approved version of the investigative plan.

B. Standards. Reserved for all standards considered during the investigation.

7.6.1.4. Folder 04 – Evidence. Reserved for all relevant evidence gathered while conducting the investigation. The evidence folder is divided into the following subfolders.

A. Interviews. Reserved for folders per every interviewee. This includes subjects, complainant, witnesses, and subject matter experts. Each interview folder should include the original transcription, the verified transcription or memorandum for record of the interview, recorded testimony file, the interrogatory, and the coordination e-mail related to the interview.

B. Documentary Evidence. Reserved for all relevant evidence gathered in the investigations.

C. Analytical Data. Reserved for documentation or files used to analyze the evidence. Example of analytical data include Chronologies, CaseSoft Suites files, and spreadsheets.

7.6.1.5. Folder 05 – Reports. Reserved for all files relevant to the ROI. The cited and redacted ROIs provided to Members of Congress, complainant, or outside of DoD under FOIA will be placed in the parent folder (not a subfolder). In oversight cases, this folder will have the Component IG's ROI and attachments. The Reports folders is further divided into the following subfolders.

A. Report References. Reserved for the documents cited in the ROI. All of the documents in this folder should be in .pdf.

B. Legal Review. Reserved for all relevant documentation or files relevant to the legal review of the ROI.

C. Preliminary Conclusions Letter and Preliminary Report. Reserved for the Preliminary Conclusions Letter, the red box, the redacted version of the ROI, and the subject's response to the Preliminary Conclusions Letter.

7.6.1.6. Folder 06 – Correspondence. Reserved for correspondence. This includes correspondence from subject matter experts, all requests for information, and updates. This folder contains the following subfolders.

A. Notification Letters. Reserved e-mails relevant to the investigations. Examples include RFIs and Coordination e-mails, 180-day letters (§ 1034 and § 4701 WRI cases only), and letters to Members of Congress.

B. Closure Memos & Letters. Reserved for the closure memorandums and letters to the Component IGs, management officials, subjects or RMO subjects, and complainants.

7.6.1.7. Folder 07 – Office of Review. Reserved for when the Military Departments join D-CATSe.

7.6.1.8. Folder 08 – Office of Approval. Reserved for the signed oversight closure document and the e-mail to the Component IG transmitting the oversight closure document. In WRI

only, also place a copy of the oversight worksheet sent to the Component IG with the closure document.

7.6.1.9. Folder 09 – Corrective Actions & Remedies. Reserved for responses from the Military Department or organization regarding corrective action taken and remedies.

7.6.1.10. Folder 10 – Internal Controls. Reserved for the Quality Assurance Review Checklist, Internal Controls Checklist, and Case Summary and Internal Control Report.

7.6.2. Additional Subfolders. Any additional electronic subfolders should be plainly labeled for ease of search and retrieval.

7.6.3. Final Case File Review. Investigators bear the primary responsibility for the data and documentation found in the case file. At case closure, the investigators will ensure that investigative data and documentation are complete using the internal controls checklist. The master file and additional folders must be organized, properly annotated, and complete. The case file must be suitable for review by an outside audit, peer review team, or oversight authority.

7.6.3.1. Documents to Preserve in the Case File. It is the investigator's responsibility to ensure that all evidence used to support the findings of the investigation is maintained in the final case file. It is also important for the investigator to ensure that official documents are preserved in accordance with DoDI 5015.02, "DoD Records Management Program," February 24, 2015 (Incorporating Change 1, August 17, 2017), which implements the National Archives and Records Administration guidelines. DoDI 5015.02 provides the following helpful guidance.

Official records are defined as "all recorded information, regardless of form or characteristics, made or received by a federal agency under federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations or other activities of the USG because of the informational value of the data in them." All official records will be included in D-CATSe under Documents.

Electronic mail (e-mail) records are defined as "senders'" and "recipients'" versions of electronic mail messages that meet the definition of Federal records, and any attachments to the record messages after they have been copied to an official recordkeeping system, paper, or microform for recordkeeping purposes." The e-mails should then be deleted from the e-mail system after they have been transferred to D-CATSe under Documents (Folder 6A).

The investigator will identify those e-mails that are considered official records and ensure that they are placed in D-CATSe under Documents (Folder 6A). This includes e-mails that are sent as official notifications or communications with the subjects, complainants, or other officials throughout the investigation; internal e-mails relating to the investigation between DoD OIG personnel; and e-mails collected as evidence during the investigation.

Official record copies of documents should reside with the official case file in D-CATSe and not be stored in personal folders. Investigators should ensure that they do not have the only copy of an official record relating to the investigation on their personal drives. Care should be exercised in this process so that the original and copy of the documents are preserved.

Versions of the report of investigation located in D-CATSe version history will be saved and maintained as official records in the electronic case file.

7.7 Data

It is critical that investigators ensure that data fields are complete and accurate. CIGIE professional standards cite the types of data that should be maintained as including the following.

7.7.1. Workload Data. Number of complaints handled, cases opened, cases closed, cases pending (active), referrals to other investigative agencies.

7.7.2. Identifications Data. Dates (allegation received, case opened, case referred, case closed), source of information, types of violations, category of investigation, subject of investigation.

7.7.3. Investigative Results. Disciplinary, remedial or other corrective actions, indictments, convictions, recoveries, restitutions, fines, settlements, savings, suspensions, debarments, recommendations to agency management.

7.7.4. Investigative Timelines. Dates for intake and investigation events. For investigation events, both planned and actual milestones through the closed date.

7.7.5. Place in Closed Pending Followup Status. Status of closed substantiated cases for which corrective actions are recommended.

7.7.6. Supervisor Case File Review. Supervisors will review the investigative data and case file to ensure that the data and documentation are complete. Supervisors will initial the internal controls checklist, providing auditable evidence that they performed a supervisory review.

7.7.7. Internal Controls Review. Investigative analysts or support specialists will perform internal controls tests on a quarterly basis. The Investigative Support Specialist (ISS)will use the internal controls checklist and perform an additional review of the investigative data and case file for currency, accuracy, and completeness. The results of the quarterly tests will be consolidated, reviewed by management to identify trends or systemic issues in information management, and reported at the DoD OIG quarterly performance briefings given to the Inspector General.

7.8 Release of Records

ODIG AI records may be requested by a variety of public or private sources. Investigators have a responsibility to safeguard IG records with respect to individual privacy, official use and other handling restrictions, and classified material. Documents may only be released in accordance with authorized procedures and applicable laws and regulations.

7.8.1. Requests under the FOIA/Privacy Act. All requests for copies of investigative records will be to the DoD OIG FOIA office. Electronic requests can be sent to FOIArequests@dodig.mil. Written requests can be addressed to:

Department of Defense Office of Inspector General
ATTN: OGC/FOIA
4800 Mark Center Drive, Suite 10B24
Alexandria, VA 22350-1500

The FOIA office will coordinate the FOIA request with the ODIG AI ISS for documents that are responsive to FOIA requests. The FOIA office will redact information from requested documents consistent with exemptions provided in the FOIA. The investigator will alert the FOIA office of any unique aspects of a case, including information that requires special handling or that should not be released to the public.

7.8.2. Release of Transcripts. Requests by witnesses for copies of their testimony should be submitted in writing to the FOIA office. The FOIA office will redact the transcript as appropriate for release. Transcripts may not be released until the investigation is completed to control the release of information and preserve the integrity of the ongoing investigation.

7.8.3. Requests within the DoD for Official Purposes. ODIG AI ROIs, including underlying documentation, may be released within the DoD for official use purposes.

7.8.3.1. Reports and underlying documentation generally need not be redacted when provided for official use. However, to protect witnesses and source sensitive information, redactions may be warranted and reports should be marked with the official DoD IG restrictive handling guidance.

7.8.3.2. When disciplinary action is planned as a result of an ODIG AI investigation, all requests for supporting documentation from the case file, in addition to materials already released to management officials appended to the ROI or in the Report of References, must be referred to the DIG AI for approval. The decision to release these materials to management or the subject will be made after consultation with the OGC and carefully weighing the level of the disciplinary action being considered (that is, termination from employment or removal from position down to reprimand or counseling), the individual rights to due process for the employee facing disciplinary action, and the inherent responsibility of the ODIG AI to protect complainants and sources of information under the IG Act.

7.8.4. Congressional Requests. Congressional requests for documents will be referred to the OLAC Director. In most cases, a written request from the Member of Congress is required. Depending on the nature of the request, a Member of Congress may be provided either unredacted material, or information redacted for public release (see section 7.4, Congressional Inquiries).

7.8.5. Requests from Other Federal Agencies. Representatives from other Federal agencies may review ODIG AI files in an official capacity in ODIG AI office workspaces as provided for in the DoD OIG Federal Register Notice of Routine Uses. Requests to review and to obtain copies must be presented in writing.

7.8.6. Media Queries. Investigators should refer requests for information from any media source (such as television, radio, newspaper, and news magazines) to the OLAC, Chief of Public

Affairs (Public.affairs@dodig.mil). ODIG AI staff will not provide information directly to a member of the media.

7.8.7. Release in Response to Subpoena. In rare cases, ODIG AI files may be requested under subpoena or other judicial order. In such cases, the release is coordinated by the OGC. In general, the ODIG AI investigator is responsible for reviewing the case files, gathering all documents responsive to the subpoena, date stamping the documents, and retaining a copy of all documents released.

CHAPTER 8—INVESTIGATIVE OVERSIGHT

8.1. Oversight Authority

8.1.1. Professional Standards. The third general standard of the of CIGIE "Quality Standards for Investigations" is "Due Professional Care." Due professional care must be used in conducting investigations and preparing related reports. Elements of due professional care include independence, objectivity, thoroughness, documentation, timeliness, and legal sufficiency.

8.1.2. Authorities

8.1.2.1. The IG Act, Section 8(c). The DoD IG will:

- initiate, conduct, and supervise such audits and investigations in the Department of Defense (including the Military Departments) as the Inspector General considers appropriate; and
- provide policy direction for audits and investigations relating to fraud, waste, and abuse, and program effectiveness.

8.1.2.2. DoDD 5505.06. The DoD IG will:

- provide oversight, as the DoD IG deems appropriate, on investigations conducted by the other DoD Components into allegations against senior officials.

8.1.2.3. DoDD 7050.06. The DoD IG will:

- review determinations by Component IGs that investigation of an allegation is not warranted;
- notify the DoD Component IG of approval or concerns;
- review the results of investigations into violations of restrictions and reprisals conducted by DoD Component IGs;
- Approve the results or ensure the DoD Component IG corrects inadequacies or initiates a followup investigation; and
- notify the DoD Component IG of approval.

8.1.2.4. Section 1034, title 10, United States Code.

- Subsection (c)(3)(E) provides that in the case of an investigation under subparagraph (D) within the DoD, the results of the investigation will be determined by, or approved by, the DoD IG.
- Subsection (c)(5) provides that the DoD IG will ensure that the IG conducting the investigation of an allegation under this subsection is outside the immediate

chain of command of both the member submitting the allegation and the individuals alleged to have taken the retaliatory action.

- Subsection (d) provides that upon receiving an allegation under subsection (c), the IG receiving the allegation will conduct a separate investigation of the information that the member making the allegation believes constitutes evidence of wrongdoing (as described in subparagraph (A) or (B) of subsection (c)(2) if there previously has not been such an investigation or if the IG determines that the original investigation was biased or otherwise inadequate.

8.1.2.5. Presidential Policy Directive 19 (PPD-19). Part 1 of PPD-19 requires that if a Part 1 reprisal complaint is filed with a DoD Component IG, the DoD IG will receive notification from the DoD Component IG of all reprisal allegations from DCIPS employees, and will review and approve the determination by a DoD Component IG that investigation of an allegation submitted to that Component is not warranted.

It also requires that the DoD IG expeditiously initiate or request the DoD Component with a statutory IG to initiate an investigation when the DoD IG determines that sufficient evidence exists to warrant an investigation. When the DoD IG requests a Component with a statutory IG to conduct an investigation, ensure that the IG conducting the investigation is outside the supervisory chain of the employee submitting the allegation or allegations as well as the individual or individuals alleged to have taken the reprisal action. The DoD IG must also review and approve the results of investigations conducted by DoD Component statutory IGs or initiate a followup investigation to correct inadequacies or ensure that the DoD Component statutory IG corrects them.

Lastly, the DoD IG must ensure the standards of proof applied in the investigation are a preponderance of the evidence for establishing that a protected disclosure was a factor in the personnel action and clear and convincing evidence for establishing that the action would have occurred absent the protected disclosure.

8.2. Oversight Review Process

WRI and ISO are referred to as Office of Approval in D-CATSe. The WRI and ISO investigators perform oversight reviews pursuant to DoD IG authorities previously cited in this chapter. Investigators will review intakes and investigations conducted by the DoD Component IGs. Investigators will use the following definitions in performing oversight reviews.

8.2.1. Definitions.

8.2.1.1. Intake. The initial complaint evaluation and clarification process to determine whether a complaint contains *prima facie* allegations of whistleblower reprisal or credible allegations of misconduct by senior officials and whether the complaint will be dismissed or investigated. The WRI intake process is limited to analysis of the alleged protected communications or disclosures and personnel actions, and analysis of whether the alleged facts, if proven, would raise the inference of reprisal, with a clarification interview of the complainant, if needed. The ISO intake process is limited to an interview of the complainant (if known) and a small collection of documents.

8.2.1.2. Investigation. The investigative activity and steps to ensure that allegations are thoroughly and objectively resolved. Investigations include conducting interviews of complainants, witnesses, and subjects; collecting documentary and other evidence; and documenting findings and conclusions in written reports that have been found legally sufficient.

8.2.1.3. Initial Oversight Review. The quick review, upon receipt of an intake or investigation from a Component IG, to determine whether significant deficiencies in the work submitted, such as the lack of an interview of the complainant or, for investigations, of the subject, would require that it be returned for further work.

8.2.2. Review of Dismissals.

8.2.2.1. WRI. WRI investigators will review intakes from the Military Departments or Defense agencies (hereafter referred to as DoD Components) that recommend dismissal of the complaint to determine if the intake adequately addressed the elements of a *prima facie* determination as set forth in the "Guide to Investigating Military Whistleblower Reprisal and Restriction Complaints," April 18, 2017.

- Alleged PCs. Determine if the alleged PCs were properly identified, if any alleged PCs were not addressed that should have been included in the intake, or both. For PCs that were not properly identified, document in writing why they were not properly identified in the context of the statute and regulation. For PCs that were missed, document them and explain why they would or would not affect the outcome of the analysis. Also document any missed or not properly identified PC as a deficiency and explain if the deficiency warrants returning the dismissal request for additional intake effort or investigation.

- Alleged PAs. Determine if the alleged PAs were properly identified, if any alleged PAs were not addressed that should have been included in the intake, or both. For PAs that were not properly identified, document in writing why they were not properly identified in the context of the statute and regulation. For PAs that were missed, document them and explain why they would or would not affect the outcome of the analysis. As part of this analysis, determine if the intake properly identified the subject involved in the PA. Also document any missed or not properly identified PAs as a deficiency and explain if the deficiency warrants returning the dismissal request for additional intake effort or investigation.

- Knowledge. Determine if the intake addressed whether the subject knew of the PC and the timing of when the subject knew of the PC, and when the subject took, withheld, or threatened the PAs.

- Inference of Causation. Determine if the intake addressed whether there was an inference of causation between the PC and the PA. Identify whether the dismissal addressed why the complainant believed the subject took, withheld, or threatened the PA in reprisal for the PC; the motive the subject had to reprise against the complainant; and the reasons the complainant stated the subject took, withheld, or threatened the action.

8.2.3. Investigations. WRI and ISO investigators assigned to the oversight branch are responsible for reviewing ROIs submitted by DoD Components. Investigators will complete an oversight worksheet for each investigation they review. The worksheets will serve as a written record of the results of the investigators' review, and will be provided to DoD Component investigators as a means to communicate feedback on the quality of their work. Accordingly, investigators will adhere to CIGIE standards in reviewing investigations conducted by DoD Component investigators; they will remain objective and professional in their written oversight worksheets; and they will not allow conjecture, unsubstantiated opinion, bias, or personal observations or conclusions to affect their work.

8.2.4. Oversight Analysis. Investigators will thoroughly review the ROI or recommended closure without investigation. Investigators will review the reports for adherence to the CIGIE professional standards for due professional care.

For each CIGIE standard, investigators will document in writing whether the standard is met, whether there are deficiencies, and whether the deficiencies are significant such that they adversely affected the outcome of the investigation. Investigators will use the CIGIE standards and their professional judgment in determining one of the following courses of action:

- The investigation was conducted in a manner consistent with CIGIE standards in all aspects—approve the investigation for closure;

- The investigation contained deficiencies that did not adversely impact the overall outcome or adequacy of the investigation—approve the investigation for closure; or

- The investigation contained a significant deficiency or multiple deficiencies that adversely affected the outcome or adequacy of the investigation—do not approve the investigation for closure until all deficiencies are resolved.

Investigators will document the results of their review in writing and in sufficient detail to create a clear record of the analytical process and decision-making. It is critical that investigators document why deficiencies did or did not affect the outcome, the adequacy of the investigation, or both.

8.2.4.1. Independence.

- Was the investigator outside the immediate chain of command of the individual making the complaint and the individual or individuals alleged to have engaged in misconduct or reprisal activity? or

- Was the investigator at least one organization higher in the chain of command than the organization of the individual making the complaint and the individual or individuals alleged to have engaged in misconduct or reprisal activity? If deficiencies exist, did they adversely affect the outcome or adequacy of the investigation? Explain why.

8.2.4.2. Due Professional Care.

a. Objectivity.

- Was the evidence gathered and reported in an objective and impartial manner?
- Were interviews conducted in an impartial and unbiased manner?
- Was the report written in an objective manner and without conjecture, unsubstantiated opinion, bias, or personal observations or conclusions?
- If deficiencies exist, did they adversely affect the outcome or adequacy of the investigation? Explain why.

b. Thoroughness.

- Was the complainant (if known) interviewed?
- Were the witnesses with knowledge of the matters under investigation interviewed?
- Was the subject interviewed?
- Were the relevant documents obtained (including e-mails)?
- Were all of the allegations addressed by the investigation?
- Were the conclusions supported by the facts?
- Was the evidence and the credibility of witnesses properly weighed?
- If deficiencies exist, did they adversely affect the outcome or adequacy of the investigation? Explain why.

c. Documentation.

- Were the findings and the conclusions in the report supported by the evidence?
- Was the witness testimony supported by interview transcripts?
- Was the documentation supporting the investigation adequate and complete?
- If deficiencies exist, did they adversely affect the outcome or adequacy of the investigation? Explain why.

d. Timeliness.

- Was the investigation conducted in accordance with statutory and regulatory timeframes as well as established performance goals?
- Were notifications made in accordance with statutory and regulatory notifications?
- If deficiencies exist, did they adversely affect the outcome or adequacy of the investigation? Explain why.

e. Legal Sufficiency.

- Were the appropriate standards and/or statutory authorities applied?
- Was the report reviewed for legal sufficiency and found to be legally sufficient?
- Were there any inconsistences between the legal review and the report findings or conclusions?
- If deficiencies exist, did they adversely affect the outcome or adequacy of the investigation? Explain why.

8.2.4.3. Oversight Approval and Disapproval Recommendations. Investigators will submit their completed oversight worksheets to the SI with recommendations regarding disposition of the case.

If the investigator determines that the intake or investigation was conducted in a manner consistent with CIGIE standards, the investigator will submit the completed oversight worksheet to the SI with a recommendation to approve the closure of the investigation. The SI will submit a draft approval letter to the Branch Chief for signature.

If the investigator has questions regarding the sufficiency of evidence or the validity of the conclusions, the investigator should contact the Component IG in an attempt to resolve the questions.

8.2.4.4. In intakes or investigations that contain a significant deficiency or multiple deficiencies that adversely affected the outcome or adequacy of the investigation, the investigator will request a roundtable discussion with the SI, the Branch Chief, and the OGC to determine the way forward. If the errors cannot be corrected by the oversight review, the SI will notify the Component IG of the deficiencies and request corrections. If the Component IG is not responsive, the investigator will prepare a letter for Branch Chief signature that will return the case to the Component for additional investigation. In all situations, these actions will be documented in the AI case notes field in D-CATSe. After the Component resubmits the intake or investigation for approval, the investigator will complete the oversight worksheet, ensuring that any remaining deficiencies are identified.

8.2.4.5. In military reprisal cases, investigators must draft a memorandum to the Component IG indicating approval of their conclusions in the case. (Refer to the "Guide to

Investigating Military Reprisal and Restriction Complaints.") Reprisal and restriction cases investigated by the Military Department IGs under 10 U.S.C. § 1034 are not closed until the DoD IG reviews and approves the investigative work, and the complainant is notified of the results. Therefore, it is necessary to provide written notification to the Military Department IG after the oversight review process is complete.

8.2.4.6. Upon completion of the oversight review process, the ISS who processes the closure will provide the Component IGs with copies of the oversight worksheet. This feedback to the Component IGs will provide a rating of the quality of individual cases in addition to valuable information on trends in systemic deficiencies in investigations within their Components. Closure forms should note discrepancies phrased in "teach and train" language to inform and provide educative guidance.

8.3. Documenting the Oversight Process

D-CATSe is the system of record used to document the oversight of Component IG recommendations. All documentation affecting the final oversight decision and supporting case data will be saved in SharePoint case files according to the published D-CATSe procedures.

8.4. Monitoring the Status of DoD Component Investigations

The Oversight Teams are responsible for monitoring the status of the investigations being conducted by the DoD Components to ensure they are completed in accordance with statutory timeframes, established suspense dates, or both.

8.4.1. Inventories. The Oversight Teams will reconcile inventories of all open cases, including investigations being conducted by the DoD Components, cases with the DoD IG pending oversight review, and cases pending followup actions (notification of closure to complainant, command actions, and remedies). The reconciliation will verify that the identifying data is correct for all cases, including DoD IG and Component IG case numbers and complainant and subject names.

8.4.2. 180-Day Notices. For military reprisal cases, WRI will notify each Component monthly of cases that D-CATSe indicates have been open 150 days or longer. This notification will remind the Component IG to submit the required 180-day notification letter if the case will not be closed within 180 days of filing, and also every 180 days thereafter until the transmission of the report, as established in DoDD 7050.06.

8.4.3. Followup and Documenting Corrective Actions. Investigators will ensure that the appropriate data fields for followup are populated in D-CATSe when the ROI contains recommendations for remedies and corrective actions. The Oversight Branch Chief will routinely monitor cases that require followup to obtain information on the remedies and corrective actions. The Oversight Branch will ensure that remedies and corrective actions are documented in D-CATSe. This process includes removing the case from followup status, entering the corrective action data, and placing the documentation of the corrective action in the system.