JULY 30, 2020

Administrative Investigations Manual

Office of the Deputy Inspector General for Administrative Investigations

A Model Oversight Organization in the Federal Government

Contents

CHAPTER 1 - INTRODUCTION 4

1.1 Purpose 4
1.2 Authority 4
1.3 ODIG-AIG Vision, Mission, and Authorities 5
1.4 Organization 8
1.5 The Council of the Inspectors General on Integrity and Efficiency 9
1.6 Recusals 10

CHAPTER 2 – COMPLAINT INTAKE 12

2.1 Sources of Complaints 12
2.2 Case Initiation 12
2.3 Informing Chain of Supervision of High Interest Matters 26
2.4 Notification of Initiation or Declination of an Investigation 26

CHAPTER 3 - PLANNING INVESTIGATIONS 27

3.1 Investigative Plan 27
3.2 On-Site Field Work 31
3.3 Investigative Tools 31

CHAPTER 4 - CONDUCTING INVESTIGATIONS 34

4.1 Introduction 34
4.2 Professional Quality Standards 34
4.3. Elements of the ODIG-AI Investigative Process 35
4.4. Documentary Evidence 36
4.5. Access to Records 38
4.6. Experts and Other Sources of Assistance 40
4.7. On-Site Field Work 41

CHAPTER 5 – INTERVIEWS 43

5.1. Introduction 43
5.2. Interview Process 43
5.3. Rights and Obligations of Witnesses 45
5.4. Witness Confidentiality 47

5.5. Authority to Administer Oaths 47
5.6. Sworn Recorded Testimony 48
5.7. Interview Techniques 50
5.8. Privileged Information 50

CHAPTER 6 - FINAL REPORTS 52

6.1. Introduction 52
6.2. Professional Standards Guidelines 52
6.3. Report of Investigation 53
6.4. Quality Assurance Review Process 57
6.5. Report Approval 59
6.6. Tentative Conclusion letters 60

CHAPTER 7 - CASE CLOSURE 61

7.1 Introduction 61
7.2 Case Closure Process 61
7.3 Closure Correspondence 61
7.4 Congressional Inquiries 63
7.5 Information Management 64
7.6 Case File Organization 65
7.7 Data 67
7.8 Release of Records 68

CHAPTER 8 - INVESTIGATIVE OVERSIGHT 70

8.1. Oversight Authority 70
8.2. Oversight Review Process 71
8.3. Documenting the Oversight Process 76
8.4. Monitoring the Status of DoD Component Investigations 76

CHAPTER 1 - INTRODUCTION

1.1 Purpose

1.1.1. This Policies and Procedures Manual provides guidance to members of the Department of Defense Office of Inspector General (DoD IG), 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 Department of Defense Hotline (DoD Hotline). The guidance ensures that investigators and administrative investigations adhere to the Quality Standards for Investigations established by the Council of the Inspectors General on Integrity and Efficiency (CIGIE). The standards are summarized in Section 1.5 of this chapter, 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 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 IG draws authority from the Inspector General Act of 1978, as amended (IG Act). Principal authorities under the Act that relate to 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 which 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) shall not, after receipt of a complaint or information from an employee, disclose the identity of the employee without the consent of the employee, unless the

Inspector General determines such disclosure is unavoidable during the course of the investigation; 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 5106.01. The authorities vested in the Inspector General, Department of Defense under the IG Act, are further implemented in the Department of Defense under DoD Directive 5106.01, "Inspector General of the Department of Defense," dated April 20, 2012.

1.3 ODIG-AIG Vision, Mission, and Authorities

The ODIG-AI vision. Engaged oversight professionals dedicated to improving the DoD.

The ODIG-AI mission. AI investigates and oversees DoD Component investigations of allegations of misconduct by senior DoD officials, and allegations of whistleblower reprisal and restriction from communication with an Inspector General or Member of Congress. AI also provides a confidential DoD Hotline for reporting fraud, waste, and abuse and for detecting and preventing threats and danger to the public health and safety of the DoD.

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 DoD Directive 5505.06, "Investigations of Allegations Against Senior DoD Officials," dated June 6, 2013.

1.3.1.1. DoD Directive 5505.06. Under DoD Directive 5505.06, ISO is charged with responsibilities including: (1) receiving allegations against senior DoD officials; (2) notifying the DoD Components whether DoD IG 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 1320.4. ISO is also responsible for performing checks of its investigative files under DoD Instruction 1320.4, "Military Officer Actions Requiring Presidential, Secretary of Defense, or Under Secretary of Defense for Personnel and Readiness Approval or Senate Confirmation," dated January 3, 2014. Under DoD Instruction 1320.4, 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 and 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 (U.S.C.) and their corresponding implementing regulations, and Presidential Policy Directive 19 (PPD-19) and its implementing regulations. The DoD IG is required by Federal statutes and Directives to review, investigate, and perform oversight of investigations of whistleblower reprisal cases as follows.

1.3.2.1. Title 10, U.S.C. Section 1034 (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 military members in reprisal for making or preparing or being perceived as making or preparing any lawful communications with a Member of Congress or an Inspector General. The statute also protects military members who make, prepare, or are perceived as making or preparing certain communications to a member of a DoD audit, inspection, investigation, or law enforcement organization, any person or organization in the chain of command, a court-martial proceeding, or any other person or organization designated pursuant to regulations or other established administrative procedures for such communications.

Communications protected under 10 U.S.C. § 1034 include information reasonably believed to evidence a violation of law or regulation, including a law or regulation prohibiting rape, sexual assault, or other sexual misconduct in violation of Articles 120 through 120c of the Uniform Code of Military Justice (UCMJ), sexual harassment or unlawful discrimination; gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety; or a threat that indicates a member's or federal employee's determination or intent to kill or cause serious bodily injury to members or civilians or damage to military, federal or civilian property. 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, military members are expected to file complaints of reprisal within one year of the personnel action occurring. Finally, the statute prohibits restricting members of the armed forces from lawfully communicating with a Member of Congress or an Inspector General. DoD Directive 7050.06, "Military Whistleblower Protection," dated April 17, 2015, implements the statute. (10 U.S.C. § 1034 and DoD Directive 7050.06). For more information about investigating 10 U.S.C. § 1034 complaints, see the Guide to Investigating Military Whistleblower Reprisal and Restriction Complaints.

1.3.2.2. Title 10, U.S.C. Section 1587 (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. DoD Directive 1401.03, "DoD Nonappropriated Fund Instrumentality (NAFI) Employee Whistleblower Protection," dated June 13, 2014, implements the statute. (10 U.S.C. § 1587 and DoD Directive 1401.03)

1.3.2.3. Title 10, U.S.C. Section§ 2409 (10 U.S.C. 2409). "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 to 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 or grand jury; or a management official or other employee of the contractor or subcontractor who has the responsibility to investigate, discover, or address misconduct.

Disclosures protected under 10 U.S.C. § 2409 include information reasonably believed to evidence gross mismanagement of a DoD contract or grant; 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 an abuse of authority relating to a DoD contract or grant.

Absent extraordinary circumstances, defense contractor or subcontractor employees are expected to file complaints of reprisal within 3 years of the alleged retaliatory action occurring. 10 U.S.C. § 2409 does not apply to Intelligence Community Element contractors or subcontractors. Defense Federal Acquisition Regulation Supplement (DFARS), subpart 203.9, "Whistleblower Protections For Contractor Employees," (added February 28, 2014), implement the statute. (10 U.S.C. 2409 and amendment, and FAR subpart 3.9 and DFAR subpart 203.9.)

1.3.2.4. Presidential Policy Directive 19. 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 (to include civilian employees, military 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.

Under Parts A or B, protected disclosures include 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; a substantial and specific danger to public health or safety; the exercise of any appeal, complaint, or grievance with regard to the violation of Section A or B of PPD-19; lawfully participating in an investigation or proceeding regarding a violation of Section A or B of this directive; or cooperating with or disclosing information to an Inspector General, in accordance with applicable provisions of law in connection with an audit, inspection, or investigation conducted by the Inspector General. Such disclosures must be made to a supervisor in the employee's direct chain of command up to and including the head of the employing agency; the Inspector General of the employing agency or Intelligence Community Element; the Director of National Intelligence; the Inspector General of the Intelligence Community; or an employee designated by any of the above officials for the purpose of receiving such disclosures.

Additionally, protected disclosures include reporting "matters of urgent concern" to Congress via the DoD IG. Matters of urgent concern are defined as serious or flagrant problems, abuse, or violation of law or executive order; deficiencies relating to the funding, administration, or operations of an intelligence activity involving classified information (but not including differences of opinion on public policy matters), and false statements to or willful withholding from Congress on an issue of material fact relating to funding, administration, or operation of an intelligence activity. Directive-Type Memorandum (DTM) 13-008, "DoD Implementation of Presidential Policy Directive 19" (February 9, 2016) implements PPD-19 within DoD.

1.3.2.5. Title 5, U.S.C. Section 2302 (5 U.S.C. § 2302) and the IG Act. The United States Office of Special Counsel has primary jurisdiction to investigate complaints of reprisal filed

by civilian appropriated fund employees throughout the Executive Branch, to include 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 DoD Directive 5106.01, 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), "Prohibited personnel practices."

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

1.3.3.1. DoD Instruction 7050.01. Under DoD Instruction 7050.01, the DoD Hotline has the authority to task DoD Components and internal DoD IG Components with resolving the Hotline complaints through investigation, audit, or other means, and providing the Hotline with the results in a Defense Hotline Completion Report.

1.4 Organization

1.4.1. DoD IG. The DoD IG 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 IG organizational structure is comprised of the Inspector General, the Principle Deputy Inspector General, the Chief of Staff, and the Deputy Inspectors General for Administrative Investigations, Audit, Investigations (Defense Criminal Investigative Service), Intelligence and Special Program Assessments, Policy and Oversight, Special Plans and Operations, and Overseas Contingency Operations. The components that provide support include the Office of Legislative Affairs and Communications and the Mission Support Offices of Strategic, Planning, and Innovation, Human Capital Management, Chief Information Office, Security, and Financial Management Office, Communications, Security (not all listed here) , and other supporting functions.

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

1.4.2. ODIG-AI. The ODIG-AI is comprised of the ISO, WRI, DoD Hotline, and Front Office Staff.

1.4.3. ISO. The ISO Directorate is responsible for conducting investigations into allegations against senior officials of the DoD and performing oversight of senior official investigations conducted by the Military Services 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 Presidential appointees. ISO also performs checks of investigative records on 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 is responsible for objectively and thoroughly conducting (or providing oversight of Service/Component IG investigations) investigations into allegations of whistleblower reprisal or restriction under the authorities pertaining to Military Service members, appropriated and nonappropriated fund employees of the DoD, employees within the DoD Intelligence Community, and DoD contractor, subcontractor, grantee, subgrantee, and personal services contractor employees.

1.4.5. DoD Hotline. The DoD Hotline Directorate is responsible for operating the DoD Hotline Program, directing its implementation in the DoD Components and for ensuring that inquiries resulting from allegations are conducted in accordance with CIGIE standards and applicable laws, regulations, and policies. The 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.

1.5 The Council of the Inspectors General on Integrity and Efficiency

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

1.5.2. General Standards

1.5.2.1. Qualifications. Individuals assigned to conduct the investigative activities of DIG-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 to 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. Establish organizational and case specific priorities and develop objectives to ensure that individual case tasks are performed efficiently and effectively.

1.5.3.2. Execution. Conduct investigations 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 their work. The investigator also has a duty to be receptive to evidence that is exculpatory, 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. Store investigative data in a manner allowing effective retrieval, referencing, and analysis.

1.6 Recusals

1.6.1. 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, and if decision is made that the person should be recused, he or she must document the recusal in the appropriate field in D-CATS, and the case will be reassigned appropriately.

CHAPTER 2 – COMPLAINT INTAKE

2.1 Sources of Complaints

2.1.1. 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, and reprisal. The Hotline staff receives complaints via a telephone hotline, the hotline public web site, and other means of communication.

2.1.2. IG Hotline Referrals. The Hotline is one of the primary sources of complaints received by ISO and WRI. On receipt of complaints, Hotline staff perform an initial screening and refer those involving allegations of whistleblower reprisal or misconduct by senior officials to ISO or WRI via the electronic case management system (Defense-Case Activity Tracking System – D-CATS).

2.1.3. Service/Defense Agency IG Notifications. The other primary source of complaints received by ODIG-AI is the notification of allegations of whistleblower reprisal or senior official misconduct from the Military Services and DoD Components through their Offices of Inspector General, Internal Review, or other channels. Notifications are required by DoD Directives 7050.06 and 5505.06.

2.1.4. Third Party Complaints. If a party alleges that someone else has been restricted or reprised against, WRI will contact the aggrieved party, if possible, in order to determine if the aggrieved party wishes to file a complaint.

2.1.5. Required Notifications. Under DoD Directive 7050.06, the Military Services are required to notify the DoD IG within 10 workdays of receiving any allegations of reprisal or restriction made by service members. Under DTM 13-008, DoD Component IGs are required to notify the DoD IG within 10 workdays of receiving any allegations of PPD-19 reprisal. Under DoD Directive 5505.06, the Component IGs are required to notify the DoD IG within 5 workdays of receiving any allegations made against senior officials.

2.1.6. Congressional Inquiries. Another source of complaints received by ODIG-AI is those forwarded by Members of Congress on behalf of a constituent or requests for investigation from Members or Committees. These complaints will be initially received and processed by the Office of Legislative Affairs and Communication (OLAC). Upon receipt, OLAC staff prepares the initial acknowledgement letter to the interested Member and refers the congressional inquiries to the appropriate DoD IG Component. Sometimes, OLAC will refer the congressional inquiries to multiple components.

2.2 Case Initiation

2.2.1. The Defense Case Activity Tracking System (D-CATS). D-CATS is an electronic case management system in use by ODIG-AI. D-CATS enables investigators and their supervisors to

perform real-time case management of investigative data and documents in an electronic, paperless environment.

2.2.2. Definitions.

2.2.2.1. Intake. The initial complaint evaluation and clarification process to determine whether a complaint contains *prima facie* allegations of whistleblower reprisal or credible allegations of non-reprisal/non-military restriction misconduct by senior officials and whether the complaint will be dismissed or be addressed by an investigation. The ISO intake process is limited in scope to an interview of the complainant (if known) and a limited collection of documents. The WRI intake process is limited to review of the complainant, analysis of the alleged protected communications/disclosures and personnel actions, and analysis of whether the alleged facts, if proven, would raise the inference of reprisal. The intake process should normally be accomplished within 30 days (for reprisal cases it is required to be accomplished in 30 days under DoDD 7050.06).

2.2.2.2. 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.

2.2.3. ISO Intake. During the ISO intake process, a brief and timely impartial analysis of an incoming complaint and determination whether it contains credible allegations of senior official misconduct that warrant investigation. The intake process is not a substitute for an investigation. It should be of limited duration and not involve extensive fact gathering. The process involves evaluating whether the complaint presents a credible allegation of senior official misconduct. An allegation of misconduct can be considered credible if it includes indications of misconduct and otherwise meets the definition in DoDD 5505.06.

2.2.3.1. Senior Official Complaint Clarification. If an incoming complaint does not convey sufficient detail to determine its credibility, ISO may conduct a complaint clarification. ISO conducts a complaint clarification interview with the complainant to obtain further information about the allegations and potential witnesses who could corroborate the complaint. Complaint clarification may also involve requesting documents, such as travel vouchers or time and attendance records.

For the ISO complaint clarification process, the Director or Deputy (DIR/DDIR) determines whether the complaint contains a credible allegation against a DoD senior official that, if proven, would constitute:

- a violation of criminal law, including the Uniformed Code of Military Justice;
- a violation of a recognized standard; or
- misconduct of concern to the leadership of the DoD or the Secretary of Defense, especially when there is an element of unauthorized personal benefit to the senior official, a family member, or an associate.

The DIR/DDIR will make the determination whether to decline, accept the case and retain it in ISO, or refer the case to a Component IG for investigation. An ISO decision to decline a complaint does not preclude other appropriate action (such as refer for audit, conduct a command climate survey, and conduct an investigation of non-senior officials).

The ISO intake process does not contemplate weighing conflicting evidence or analyzing evidence against a standard, both of which steps should move an intake review either to ISO investigation or referral to a Component IG for investigation subject to ISO oversight review upon completion, in accordance with DoDD 5505.06.

Criteria for not investigating allegations of senior official misconduct include:

- the allegations do not include a credible allegation of misconduct;
- the allegations do not include sufficient information with which to conduct a focused investigation;
- 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 (requests for relief to the Board for Correction of Military Records (BCMR), an evaluation report appeal, an Article 15 appeal, the equal employment opportunity (EEO) office, administrative grievance, requests for assistance or redress to the chain of command); or
- the allegations involve actions or events that occurred many years ago and are too old to investigate.

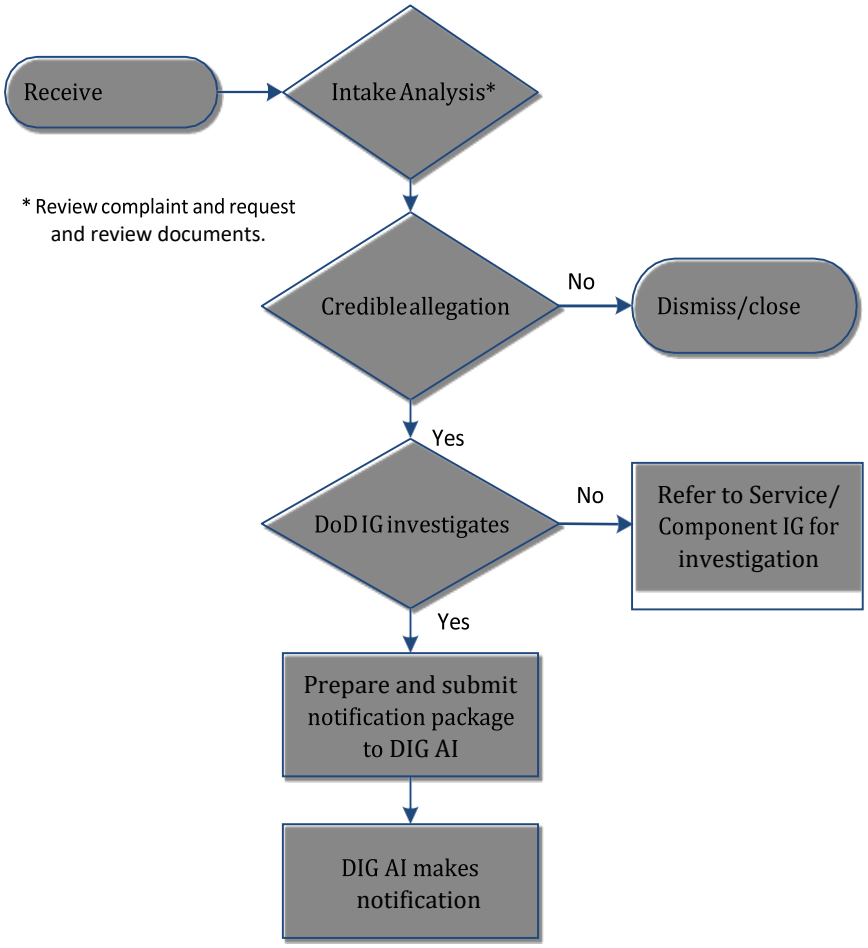
2.2.3.2. ISO Intake Workflow. Figure 2.1 shows the ISO intake workflow.

- DoD Hotline refers complaints involving senior officials in D-CATS to ISO.
- ISO intake investigator reviews the complaint with the ISO DIR/DDIR and takes one of three courses of action:

DoD Hotline refers complaints involving senior officials in D-CATS to ISO.
ISO intake investigator reviews the complaint with the ISO DIR/DDIR and takes one of three courses of action:

- decline to open an investigation;
- open an investigation and assign to an ODIG-AI investigator; or
- refer to the Component IGs for investigation.

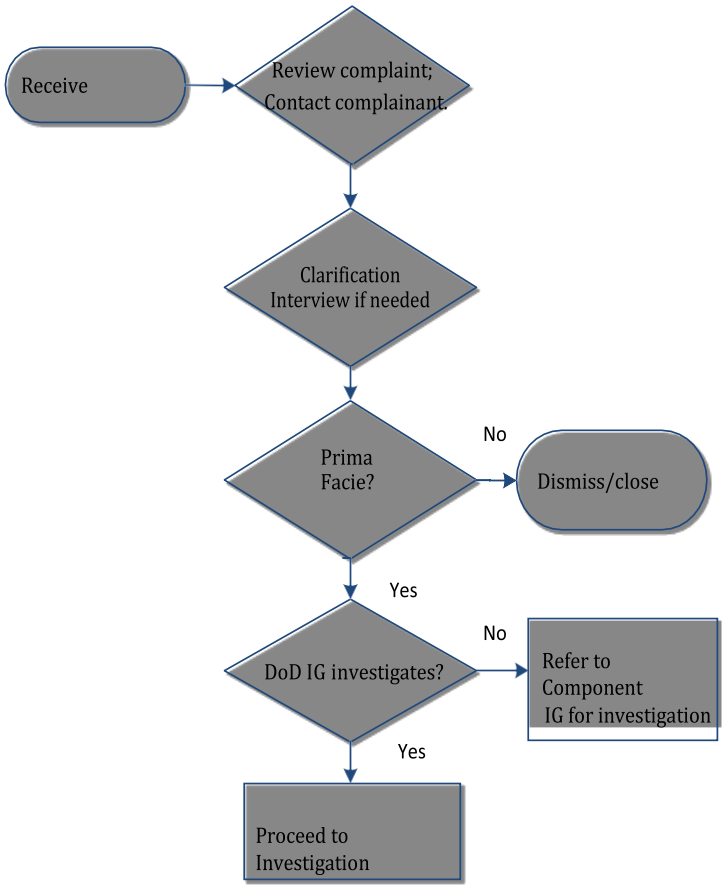
Figure 2.1. ISO Intake Workflow



2.2.4. WRI Intake. Upon receipt of a complaint in D-CATS, an Investigative Support Specialist (ISS) assigns cases for appropriate handling.

The purpose of the intake process is to determine whether complaints alleging reprisal provide sufficient evidence to warrant an investigation—that is, whether the alleged facts, if proven, would raise an inference of reprisal. The intake process includes the following steps: (1) review of the entire complaint; (2) contact to acknowledge the complaint; (3) if necessary to clarify the complaint, an intake interview of the complainant; (4) analysis of the alleged facts against the elements of reprisal (or in the case of a restriction complaint against the definition of restriction); and (5) a recommendation to the supervisor to dismiss the case without full investigation or proceed to investigation. At the intake stage, the complainant's assertions are viewed in the light most favorable to the complainant.

Figure 2.2. *WRI Intake Workflow*



2.2.4.1. The SI reviews the complaint. Unless the case is declined in accordance with the following criteria, it should be assigned to an investigator for intake. The SI should usually decline a case referred from Hotline without assigning it to an investigator for intake in the following circumstances.

- The complaint makes no explicit or implicit reference to reprisal or military restriction. IG DoD lacks jurisdiction over the complaint, or the complaint was clearly filed in the wrong forum—that is, the allegations implicate a statute or authority other than PPD-19; 10 U.S.C. sections §§ 1034, 1587, or 2409; or the IG Act.
- The complaint could be handled by the Office of Special Counsel and does not implicate persons or allege facts that, if proven, would be of interest to the IG, the Secretary of Defense, or otherwise would be of high interest, thus meriting consideration of exercising the IG DoD's discretionary authority to investigate.
- Such a vast length of time has passed since the alleged reprisal or military restriction occurred that an investigation would be impracticable.
- The Complainant filed the same allegations on an earlier date, and they are currently being clarified or investigated by the IG DoD or a DoD Component; that is, this is a duplicate complaint.
- The complaint is related to another case and contains no new and compelling

information that would warrant the reopening of a closed case or the creation of a new one.

- The complaint is a duplicate or is intrinsically related to a previously filed complaint, in which case the SI should decline the case and ask Hotline to add information as a supplement to the existing closed case.
- The matters identified in the complaint are subject to an ongoing criminal proceeding.
- The complainant did not give consent to the Hotline to release their identity within the IG DoD.
- The complainant did not provide contact information or the complaint was filed anonymously and there is no way to seek consent from the alleged aggrieved party to proceed with intake.
- The complaint, even when viewed in the light most favorable to the complainant, is frivolous.

2.2.4.2. Review of the Entire Complaint. The investigator will verify the complainant is covered by a statute administered by IG DoD; review the alleged restriction, or if reprisal, the protected communications, to whom they were made, when they were made, and any alleged prohibited personnel actions.

2.2.4.3. Acknowledgment of Complaint. As soon as practicable after case assignment, the investigator will contact the complainant to advise that the complaint has been received. Additionally, the investigator will clarify the allegations with the complainant if they are not clearly articulated in the written complaint. If a clarification interview is required, the investigator should take notes during that interview and then prepare a memorandum for the record.

The investigator may also request additional information or documentation if needed to establish timeliness or jurisdiction; in general, the burden should not be placed on the complainant to provide many documents, create a chronology, or fill out additional questionnaires developed for the purpose of clarifying their allegations.

With supervisory approval, the intake clarification interview may become the interview of record, with a prepared interrogatory and a sworn, recorded interview, especially if the complaint was filed under 10 U.S.C. §§ 2409 or 1587, or PPD-19. In such instances, the interview would include asking for information such as the names, titles, and duty locations of knowledgeable witnesses. Ask the complainant to send any available documentation pertaining to the protected communication(s) and the personnel action(s). NOTE: Investigators should exercise care when contacting the complainants, especially at their workplace, so as not to compromise their confidentiality.

2.2.4.4. Intake Worksheet. The following factors are analyzed using the intake worksheet.

Title 10 U.S.C. § 1034

Timeliness. Did the complainant file the complaint within 1 year of the date on which the complainant became aware of the personnel action? 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 personnel action, 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:

1. Was actively mislead regarding his or her rights;
2. Was prevented in some extraordinary way from exercising his or her rights; or
3. Filed the same allegation within the 1-ytear period with the wrong office or agency.

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

Does the complaint, as supplemented by the interview of the complainant, make a *prima facie* allegation by including:

1. Protected Communication. Has the complainant alleged that he or she made or was preparing to make a protected communication or was he or she perceived as having made a PC? Table 2.1, found in DoDD 7050.06, "Military Whistleblower Protection" (April 17, 2015), defines protected communication. Table 2.3 provides definitions found in DoDD 7050.06.

Table 2.1. 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 violations of Section 920 through 920c of Reference (c) (articles 120 through 120c 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 Federal Government that indicates a determination or intent to kill or cause serious injury to Service members or civilians or damage to military, federal, or civilian property; • Testimony, or otherwise participating or assisting, in an investigation or proceeding related to a communication as described above; or	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 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.

• Filing, causing to be filed, participating in, or otherwise assisting in a military whistleblower reprisal action.		

Gross Mismanagement
DoDD 7050.06, "Military Whistleblower Protection," (April 17, 2015) 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, "Military Whistleblower Protection," (April 17, 2015) 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, "Military Whistleblower Protection," (April 17, 2015) 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 Whistleblower Protection Act (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.

2. Personnel Action. Has the complainant alleged that an unfavorable personnel action was taken or threatened against him or her, or was a favorable personnel action withheld or threatened to be withheld from him or her?

Personnel Action
DoDD 7050.06, "Military Whistleblower Protection," (April 17, 2015) defines a "personnel action" as any action taken on a Service member that affects, or has the potential to affect, that member's current position or career. Such actions include promotion; disciplinary or other corrective action; transfer or reassignment; a performance evaluation; decisions concerning pay; benefits, awards, or training; relief and removal; separation; discharge; referral for mental health evaluations; and any other significant change in duties or responsibilities inconsistent with the Service member's grade.

Knowledge. Do the alleged facts support an inference that the subject had knowledge of the PC or perceived the complainant as making or preparing to make a PC?

Causation. Do the alleged facts support an inference of reprisal? That is, can a causal connection between the PC and the PA be inferred? This threshold can be met where the facts suggest the existence of one or more of the following.

- The PA followed closely behind the PC.
- The PC was about something that would give the subject motive to reprise or the subject has expressed animosity toward the PC.

- The complainant received worse treatment than others who had not made PCs.

Title 10 U.S.C. § 1587

Does the complaint, as supplemented by the interview of the complainant, make a *prima facie* allegation by including:

1. Protected Disclosure. Has the complainant alleged that he or she made or was preparing to make a protected disclosure or was he or she perceived as having made a PD?

Protected Disclosure
DoDD 1401.03, "NAFI Employee Whistleblower Protection," (June 13, 2014) defines a protected disclosure as 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, if such disclosure is not specifically prohibited by law and if the information is not specifically required by or pursuant to executive order to be kept secret in the interest of national defense or the conduct of foreign affairs; or a disclosure by an employee, former employee, or applicant to any civilian employee or service member designated by law or the Secretary of Defense to receive disclosures in accordance with 1587(b)(1) of Reference (b), which the employee, former employee, or applicant making the disclosure 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.

Mismanagement
DoDD 1401.03, "NAFI Employee Whistleblower Protection," (June 13, 2014) defines "mismanagement" as "wrongful 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, "NAFI Employee Whistleblower Protection," (June 13, 2014) 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 1401.03, "NAFI Employee Whistleblower Protection," (June 13, 2014) 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 Mismanagement
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.

2. Personnel Action. Has the complainant alleged that an employee has taken or failed to take, or threatened to take or fail to take, a personnel action against him or her?

Personnel Action (NAFI)
DoDD 1401.03, "NAFI Employee Whistleblower Protection," (June 13, 2014) 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.

Knowledge. Do the alleged facts support an inference that the subject had knowledge of the PD or perceived the complainant as making or preparing to make a PD?

Causation. Do the alleged facts support an inference of reprisal? That is, can a causal connection between the PD and the PA be inferred? This threshold can be met where the facts suggest the existence of one or more of the following:

- the PA followed closely behind the PD
- the PD was about something that would give the subject motive to reprise or the subject has expressed animosity toward the PD
- the complainant received worse treatment than others who had not made PDs

Title 10 U.S.C. § 2409

Timeliness. Did the complainant file the complaint 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?

Does the complaint, as supplemented if necessary by the interview of the complainant, make a *prima facie* allegation by including:

1. Protected Disclosure. Has the complainant alleged that he or she made a protected disclosure or was perceived as having made a protected disclosure?

Types of Disclosure	When Made To
Information reasonably believed to evidence:	• a member of Congress • a representative of a committee of Congress
• Gross mismanagement of a Department of Defense contract or grant • A gross waste of Department of Defense funds • A substantial and specific danger to public health or safety	• Inspector General • 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 violation of law, rule, or regulation related to a Department of Defense contract (including the competition for or negotiation of a contract) or grant • Abuse of authority relating to a Department of Defense contract or grant	• A court, grand jury, or any judicial or administrative hearing (as clarified in the DFAR: "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." • 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

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 *de minimis* wrongdoing or simple negligence. It does not include management decisions that are merely debatable among reasonable people.

r

Gross Waste of Funds
Case law developed under the WPA defines a "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 Safetys
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. § 2409 defines "abuse of authority" as "an arbitrary and capricious exercise of authority that is inconsistent with the mission of the DoD or the successful performance of a Department contract or grant."

2. Discharge, demotion, or other action. Has the complainant alleged that the company discharged, demoted, or took or failed to take another action with respect to him or her?

3. Contributing factor. Does timing or inferred subject knowledge support the inference that the alleged protected disclosure was a contributing factor in the discharge, demotion, or other action taken or not taken with respect to the complainant?

Contributing Factor
Any 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.

If these three factors above are present, the complaint makes a *prima facie* allegation. However, there are other ways to infer a contributing factor, such as information that goes to:

- The strength or weakness of the subject's stated reasons for taking or failing to take the action;

- Whether the PD was personally directed at the subject;
- Whether the subject had a desire or motive to retaliate against the complainant.

Thus, the investigator should also ask the complainant questions that would elicit such information, to be weighed together with the knowledge and timing factors.

Insufficient evidence to warrant investigation. If the complaint is frivolous or has previously been addressed in another Federal or State judicial or administrative proceeding initiated by the complainant, it may not warrant investigation.

Presidential Policy Directive 19 (PPD-19)

Part A. Does the complaint, as supplemented by the interview of the complainant, make a *prima facie* allegation by including:

1. Protected disclosure or activity. Has the complainant alleged that he or she made a protected disclosure or was perceived as having made a protected disclosure; 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?

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 • 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 3. Lawfully participating in an investigation or proceeding regarding a violation of Section A or B of this directive; or 4. Cooperating with or disclosing information to an Inspector General, in accordance with applicable provisions of law in connection with an audit, inspection, or investigation conducted by the Inspector General 5. Reporting matters of urgent concern:	1 – 4: • a supervisor in the employee's direct chain of command up to and including the head of the employing agency • the Inspector General of the employing agency or Intelligence Community Element • the Director of National Intelligence • the Inspector General of the Intelligence Community • an employee designated by any of the above officials for the purpose of receiving such disclosures 5. To Congress, via the DoDIG

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 *de minimis* 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 a "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 one or more of the following: • A serious or flagrant problem, abuse, violation of law or Executive Order, or deficiency relating to the funding, administration, or operations of an intelligence activity involving classified information, but does not include differences of opinion concerning public policy matters. • 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. • 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 7(c) of the IG Act, in response to an employee reporting an urgent concern.

2. Personnel action. Has the complainant alleged that he or she received a personnel action on or after July 8, 2013?

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 prior to July 8, 2013.*

3. Contributing factor. Does timing or the inference of subject knowledge support the inference that the alleged protected disclosure was a contributing factor in the actual or threatened personnel action?

If these three factors are met, the complaint makes a prima facie allegation. However, there are other ways to infer a contributing factor, such as information that goes to:

- the strength or weakness of the subject's stated reasons for taking or threatening to take the action;
- whether the PD was personally directed at the subject;
- whether the subject had a desire or motive to retaliate against the complainant.

Thus, the investigator should also ask the complainant questions that would elicit such information, to be weighed together with the knowledge and timing factors.

Part B. Does the complaint, as supplemented by the interview of the complainant, make a prima facie allegation by including:

1. Protected disclosure or activity. Has the complainant alleged that he or she made a protected disclosure or was perceived as having made a protected disclosure; 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 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 definitions for protected disclosures under Part A.

2. Action affecting eligibility for access to classified information. Has the complainant alleged that an executive branch employee with authority to do so took, directed others to take, recommended, or approved any action affecting the complainant's eligibility for access to classified information?

3. Contributing factor. Does timing or the inference of subject knowledge support the inference that the alleged protected disclosure was a contributing factor in taking, directing others to take, recommending, or approving any action affecting the complainant's eligibility for access to classified information?

If these three factors are met, the complaint makes a prima facie allegation. However, there are other ways to infer a contributing factor, such as information that goes to:

- the strength or weakness of the subject's stated reasons for taking, directing others to take, recommending, or approving any action affecting the complainant's eligibility for access to classified information;
- whether the PD was personally directed at the subject;
- whether the subject had a desire or motive to retaliate against the complainant.

Thus, the investigator should also ask the complainant questions that would elicit such information, to be weighed together with the knowledge and timing factors.

2.2.4.5. Recommendation for Intake Disposition. The investigator analyzes the factors listed above and recommends to the SI whether the complaint makes a prima facie allegation. If there is a prima facie complaint of reprisal or military restriction, the SI may refer military cases to a Component IG or a PPD-19 Part A case to a Statutory IG within the DoD Intelligence Community for investigation. NAFI reprisal, contractor/subcontractor reprisal, and PPD-19 Part B cases may not be referred outside of DoD IG for action. All decisions to dismiss

complaints or for WRI to retain complaints for investigation require WRI DIR/DDIR approval following a recommendation by the SI.

2.3 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 or public health and safety, Congressional or news media interest, or other matters deemed to be of interest to the Secretary of Defense.

2.4 Notification of Initiation or Declination of an Investigation

2.4.1. Official Notification Correspondence. Once the determination has been made to open an investigation, the assigned or intake investigator will prepare official notification correspondence. The notification procedures may vary depending on the circumstances of the case.

2.4.2. ISO Case Notification. For ISO cases, the intake investigator will prepare a memorandum to the Component IGs notifying them that the ODIG-AI is opening an investigation into allegations against one of their senior officials. In some cases, the intake investigator will also prepare a memorandum to the Secretary of Defense. The draft memorandum will be forwarded to the DIG-AI or the IG for signature. The DIG-AI will verbally notify the subject of the investigation.

2.4.3. WRI Case Notification. For WRI cases, the investigator will prepare and coordinate a notification letter to the complainant and a memorandum to the Military Service/Component Inspector General, the Office of the Secretary of Defense or the contracting officer, and defense contractor or subcontractor, grantee, or subgrantee, as required under relevant whistleblower laws and regulations. The WRI notifications will be signed by the Director WRI. In the event a case involves a subject who is a senior official, the notification will be signed by the DIG-AI after verbally notifying the subject.

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 an investigative plan to be completed and approved prior to 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 has been made to open an investigation. Investigators should schedule a roundtable discussion with the SI prior to commencing fieldwork. In ISO cases and in certain WRI cases as determined by management, the DIR/DDIR and the Office of General Counsel (OGC) attorney must also be present Good investigative plans give investigators, supervisors, and attorneys a roadmap 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 the Defense-Case Analysis Tracking System (D-CATS) 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;
- 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 of the allegations warrant investigation. This is probably the most important aspect of investigative planning. The investigator will consult with the assigned attorney to be certain that the issues that warrant investigation have been 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/or 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) in order 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 be interviewed, the questions to ask the witnesses, and the documents to be obtained.

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.

There are several things to remember 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, Service 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 Activities, or international alliance organizations such as NATO.

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, review documents that show the organizational structure and the chain of command. Know the mission/function of the organization before interviewing its members. This will assist in placing in context the information provided by witnesses. Similarly, review individual biographies (most common with senior officials) and personnel records to aid in developing 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 DoD Directive 5106.01 and DoD Instruction 7050.03, "Office of the Inspector General of the Department of Defense Access to Records and Information," March 22, 2013, OIG DoD investigators are to be granted expeditious and unrestricted access to copies of all records, regardless of classification, medium (e.g., paper, electronic) or format (e.g., digitized images, data) and information available to or within any DoD component. No officer, employee, contractor, or Service member of any DoD Component may deny the OIG DoD access to records.

Accordingly, investigators should consider the following:

- Documents. 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 affords 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 Inspector General 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] and/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 in obtaining special types of records:

- Personnel Records. Military personnel records are maintained at personnel centers for the Military Services. 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

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) may provide assistance. If the contract relates to a specific DoD facility or installation, there may be a local contracting office that can provide information. The local IG can also assist in locating the points of contact at the installation. There are several DoD and federal-level systems where contract information and documentation can be obtained. The Federal Data Procurement System (FPDS) can be searched by company name or DoD organization to obtain

contract numbers, and the Electronic Document Access (EDA) 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 DFAS Internal Review, Criminal Investigations Branch, with the following information: the document requested (such as vouchers, orders, receipts), the traveler's full name, Social Security Number (SSN), and travel date range, where the voucher was most likely filed or processed, and if the voucher was not filed under the Defense Travel System (DTS).

3.1.2.5. Witnesses. Under DoD Directive 5106.01, DoD IG 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 are helpful in identifying the titles and ranks of witnesses and where they fall in the chain of command.

3.1.2.5.1. Witness Availability. Once witnesses have been identified, 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 impact the order of witness interviews and the timing of the investigator's travel.

3.1.2.6. Travel Locations/Dates. 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, combine travel to several different locations into one trip within the same geographic area. In lieu of long distance travel for one interview, consider alternatives such as the use of video teleconferencing, web cam 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. 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. Develop a course of action that will maximize efficiency and effectiveness. However, do not become locked into the plan. 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-CATS 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-CATS the planned milestones should not be changed, and the actual milestones should be entered. If there

are processing delays that occur during the investigation, such as when waiting on records, investigators should document the reason for the delays in D-CATS.

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 OGC attorney must also be present, to discuss the facts, draft report of investigation (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-CATS is used in these meetings for participants to access all information available pertaining to a case. At a minimum, roundtables are conducted just prior to the subject interview (pre-subject) and afterwards (post- subject) to collaborate case related information.

3.2 On-Site Field Work

3.2.1 Preparation. Obtain and review as much of the documentation and e-mails as possible prior to on-site travel to assist in the selection of witnesses and the development of interview questions. At least 10 days prior to arriving on-site, make necessary local arrangements to ensure the on-site field work is effective and efficient. The local IG is normally best suited to assist with DoD IG investigations. They can assist in arranging interviews, interview locations, and access to witnesses. Most importantly, make sure 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 prior to their travel.

3.2.2.1. DTS and Travel Standards. Investigators must arrange and obtain authorization for their travel in the Defense Travel System (DTS). Investigators need to fully 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 with 5 days after returning from the trip.

3.2.2.2. Foreign Travel. Investigators must report all planned official foreign travel to the Office of Security. Consult the Foreign Clearance Guide, DoD IG Security, and DoD IG 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 IG travel support offices require 30-day advanced 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 Compensation Time Request. If travel is expected to exceed normal business hours," the investigator must complete a Travel Compensatory Time Request within 5 days of return 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 aid in the organization of the investigation and the analysis of the evidence. Offices may use

computer-based tools to assist in the organization and analysis of evidence. Other static or written forms of such tools include the following:

3.3.1. Investigation Matrix. An investigation matrix (Figure 2) is helpful in organizing the witnesses that need to be interviewed for each of the allegations being addressed by the investigation.

Figure 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 (Co-worker)	~	~	-	
Mr. Spock	X	X	X	
(Co-worker)	X	X		Was safety report filed? Was leave requested?
X = Primary witness	- = Discuss if knowledgeable		~ = Do not discuss	

3.3.2. Force-Field Diagram. A force-field diagram (Figure 3) is a valuable tool for graphically depicting the evidence, the weight of the evidence, and the preponderance of the evidence. It is a visual representation the facts that includes the allegation with standard, the elements of proof, facts to substantiate or not substantiate, and the type of evidence—direct, circumstantial, hearsay, or opinion. Take the following steps to construct a force-field diagram.

1. Begin by first writing the allegation and elements of proof at the top of the chart.

2. Next, divide evidence into two groups:
   a. Evidence in support of substantiating the allegation
   b. Evidence in support of not substantiating the allegation.

3. Indicate the type of each piece of evidence (direct, circumstantial, hearsay, opinion). Similarly, make a notation if unsworn testimony is provided (i.e., statement) versus sworn testimony. Look for multiple citations in the evidence to establish any facts, and enter the facts as a separate line in either or both of the columns. The investigator then weighs the resulting columns of evidence to determine a preponderance of evidence. Three entries of direct evidence weigh greater than three entries of hearsay evidence. Finally, assess the evidence as a whole and make a determination of substantiated or not substantiated.

Figure 3.2 Force-Field Diagram.

Allegation: Who did what in violation of which standard.

Element of Proof: List the elements of the standard.	
Substantiate	Not Substantiate
• Enter evidence here that would indicate the subject did perform the alleged impropriety • Summarize the evidence and indicate its category and level	• Enter evidence here that would indicate the subject did not perform the alleged impropriety • Summarize the evidence and indicate its category and level

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 their supervisor. Together they should to determine whether further investigative activity should be ceased and notifications should be made to the DoD IG 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 guides investigators to conduct investigations in a timely, efficient, thorough, and legal manner. 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 exculpatory, 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 in order for investigations to be credible, they must be thorough. In general, investigators should interview all material witnesses and obtain all evidence relevant to the issues under investigation. 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 IG. Investigators should routinely assess the evidence they have obtained during the course of their investigation, and consult with their supervisor 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. It is also important for investigators to stay focused on the issues and the scope identified in the investigative plan, and discuss with their supervisor how to handle new issues that are raised during the course of the investigation. Investigators must remember that the investigations they are conducting can have a profound impact on individuals' lives, professional careers and reputations, and on 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 upon 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 assists the investigator in resolving 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 Services 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 afforded to complainants and sources of information to the fullest extent permitted under 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, or subjects with firsthand knowledge of events at issue.

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

4.3.6. Subject Interviews. The subject of the investigation will always be interviewed. This affords 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 Fact Book folders in the case file. All evidence relied upon in the report of investigation will be included in the D-CATS Fact Book folder.

4.3.8. Quality Controls. Quality controls will be in place, including referencing source documents to factual statements 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, in order to ensure supportability of the findings and conclusions.

4.3.10. Tentative Conclusions. Subjects who are senior officials will be notified (either orally or in writing) of tentative conclusions where allegations are substantiated and given an opportunity to respond to the tentative conclusions prior to issuing 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 or the privacy of complainants, witnesses, and subjects under the IG Act; Privacy Act; and Freedom of Information Act.

4.3.12. Closure Letters. Subjects, complainants, Military Services Inspectors General, and Component Designated Officials, and other officials required by statute or directive, as appropriate, of 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, he or she is to obtain copies. Examples of relevant documents include, but are not limited to, 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 prior to 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 prior. 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 on-site 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, 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 within 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 log-on 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 where there is a concern about a particular system or in situations where files are password protected separately from other files.

4.4.5. Requesting Records

4.4.5.1. Telephonic 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 service or agency point of contact (POC) or directly to the organization in possession of the records. It is normally a good idea to 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 Service/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 in order for a Hotline investigator to confirm the investigator's identity.
    - An investigator should coordinate with the Hotline so that 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 where it is important to set the tone with the command or the organization that the DoD IG is conducting a formal investigation, to establish a formal written request of the documents that are requested, and to 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 Office of Inspector General, Department of Defense. The request is made under the authority of DoD Directive 5106.01, "Inspector General of the Department of Defense," dated April 20, 2012, paragraph 7.b., which states that the IG DoD shall have access to "all records (electronic or otherwise), reports, investigations, audits, reviews, documents, papers, recommendations, or other information or material available to any DoD [c]omponent."

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. DoD Directive 5106.01. DoD Directive 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. DoD Instruction 7050.03. DoD Instruction 7050.03, "Office of the Inspector General of the Department of Defense Access to Records and Information," dated March 22, 2013.

1. 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.

2. 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 [DoD Directive 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].

3. Enclosure 2, Paragraphs 2.a. and 2.b., directs that DoD Component heads shall:

Establish procedures to ensure that requests for access to records or information under authorized OIG DoD audit, investigation, follow-up, 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 IG DoD by the Component head no later than 15 business days from the date of the OIG DoD request.

4.5.1.4. If an individual resists the OIG's authority for access to information, an investigator should advise the individual that he or she should contact the local IG or staff judge advocate to confirm the DoD IG authority. In the event that the investigator cannot resolve the denial of access at the local level, he or she should immediately notify their 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," dated August 31, 2007, which implements DoD Directive 5200.l-R, "Information Security Program," dated January 1997.

4.5.2.2. Need to Know. Before granting the investigator access to classified information, the possessor of the classified information must first make a determination that the investigator has a requirement for access to the classified information in order to accomplish 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 DoD Directive 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, contact the Office of Security, Office of the Assistant Inspector General for Administration and Management.

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 a ROI, it is imperative that an investigator follow the rules governing protection and accountability of classified information. Classified information shall 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 the Inspector General Instruction 5200.1, "Information Security Program," dated August 20, 2018,

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 (IGDINST 5205.07), "Special Access and Other Sensitive Programs," dated May 6, 2003, and DoD Directive 5205.07, "Special Access Program (SAP) Policy," dated July 1, 2010.

4.5.4. Non-DoD Government Records and Records of Other Federal Agencies. The IG Act authorizes the OIG to request information or assistance from other Federal governmental agencies as may be necessary for carrying out 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, Deputy Assistant Inspector General for Audit Policy and Oversight. 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 IG Office of Investigative Policy & Oversight. Investigators should refer to IPO web site for guidance and templates for obtaining an IG subpoena (http://www.dodig.mil/programs/subpoena/subpoena.html).Experts and Other Sources of Assistance

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 in proving or

disproving the allegations. Consider obtaining assistance from a variety of experts outside of ISO and WRI when necessary. Consult with your supervisor prior to seeking this type of assistance.

4.6.2. Technical Experts

4.6.2.1. DoD Policy Experts. In cases where Service regulations are unclear or appear to conflict with DoD regulations, investigators will work with OGC to obtain a clarification of the correct policy to be applied in their case. 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 if this information is provided in writing to facilitate the OGC in rendering 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, 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. There are engineers assigned within the Office of the Deputy Inspector General for Policy & Oversight, Technical Assessment Directorate who can assist with investigations.

4.6.2.4. Auditors. Auditors are available from the ODIG-AUD (Audit). Additionally, each Service 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 DoD, and may be used to conduct audits of invoices, billings and/or 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 Service: 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 from a hard drive or removable media that was deleted or reformatted.

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 Information Systems Directorate, Chief of Staff.

4.7. On-Site Field Work

4.7.1. Arrival On-Site. On arrival at the activity, visit the local POC and ensure satisfactory arrangements have been made for witness interviews, records retrieval, and administrative and

logistical support. Check the facility provided for interviews. 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 on-site visit until they have conducted a thorough investigation. Interview new witnesses who have been identified during the course of the visit who are available locally. Similarly, 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 prior to a site visit, make efforts to meet with the complainant face-to-face if feasible to ask follow-up questions arising from newly obtained testimony or investigative leads. If necessary, extend your 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 on the investigative process which involves a rigorous review process including quality assurance and legal reviews prior to the report of investigation being approved and issued.

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, competence, and professionalism. To maintain the credibility of 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. Approach interviews with an open mind. Ask questions to get both sides of the story – exculpatory and incriminating information. Don't lead witnesses by asking questions designed to reach a preferred answer. Let the witnesses tell their side of the story.

5.1.2.2. Be Prepared. Know the objective of the interview. Know what information needs to be obtained from the interview, and the standards and the elements of proof for the conduct at question. Prepare a list of questions prior to the interview to thoroughly elicit the needed information.

5.1.2.3. Listen. Ask short, direct, open-ended questions and listen to the answers. Give the witness a chance to answer the question; don't interrupt; don't do all of the talking; let the witness talk about their knowledge of the events under investigation.

5.1.2.4. Be Respectful. Treat witnesses with dignity and respect. The investigator should treat a witness with the same respect that the investigator would like to receive if they were the one being interviewed. Don't be rude or condescending. It is permissible to challenge or confront a witness, but do not 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 identify all relevant issues and elements of proof. Then consider the facts or information necessary to resolve each of those issues. Determine which witnesses can supply needed facts or information and thus, must be interviewed. Formulate an objective for each interview and develop a line of questioning based on that objective. Consider the location of the interviews and the order in which witnesses will be interviewed. Review the complaint, biographical data on the witnesses, files and documentary evidence (such as .psts), and information on the witnesses' organization(s).

5.2.2. Selection of Witnesses to Interview. When conducting an investigation, always interview the complainant, the subject, and other primary witnesses (those having firsthand knowledge of the events at issue). 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, do not avoid witnesses who may have valuable information. When in doubt, do a screening interview to determine if the witness has pertinent information regarding the matter under investigation. If the witness has information that is needed to complete the case, proceed with a sworn recorded interview.

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

5.2.4. Line of Questioning. Under most circumstances, prepare a list of questions, or interrogatory, to ask a primary witness before conducting the interview. Anticipate possible responses and formulate follow-up 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, avoid getting locked into a prepared script. During the interview, 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. 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, conduct interviews in a quiet location away from the witness' 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.

1. 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, contact the legal offices (staff judge advocate or general counsel) and request assistance.

2. As a matter of courtesy, investigators will normally interview senior officials in their offices. 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.

3. 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 IG investigator. If necessary, arrange to interview those witnesses after duty hours at off post locations, such as public buildings, Government offices, hotel

rooms, or private residences. Always use two investigators for interviews in hotel rooms or private residences.

4. 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, take steps to ensure that the witness has sufficient privacy to discuss the issues candidly.

5.2.6. Scheduling Interviews. Unless completely impractical, initiate contact with a witness via phone call. Explain AI policy about swearing in, recording, and transcribing interviews, and the use of two interviewers. Introduce the Privacy Act notice and get the witness' e-mail address. Do not rush interviews, particularly those with the subject or the complainant. Schedule interviews to ensure sufficient time to cover all the issues and allow enough time to follow-up on unanticipated information. Allocate time for breaks (generally 5 or 10 minutes each hour). Schedule appointments with sufficient time between them so the witnesses do not encounter one another when arriving or leaving the interview site. 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, consider having the local IG provide a scheduling POC in order 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, review documents that show the organizational structure and the chain of command. Know the mission/function of the organization before interviewing its members. This will assist in placing in context the information provided by witnesses. Similarly, review individual biographies (most common with senior officials) and personnel records to aid in developing pertinent questions for each witness.

5.3. Rights and Obligations of Witnesses

5.3.1. A Witness' Protection against Self-Incrimination. DoD IG 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 IG investigation under the IG Act, and DoD Directive 5106.01. However, all employees have the Constitutional right against self-incrimination. If a witness refuses to be interviewed invoking their right against self-incrimination, the investigator should terminate the interview immediately.

5.3.2. Article 31b Warnings (Military Members). Article 31b of the Uniform Code of Military Justice (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 has issued guidance and a model Garrity warning to be used by Inspector General investigators when interviewing government employees. However, Inspectors General have discretion in determining the specific circumstances under which a Garrity warning should be given.

If investigators are planning to interview the subject of the investigation on matters that may include potential criminal violations, they should consult with their supervisor and with the OGC on whether to issue the subject a Garrity warning at the start of the interview. Factors to consider in making this determination should include whether the potential criminal violations would rise to the level of those that are prosecuted by the U.S. Attorney. Consultation with DCIS may be warranted in this regard.

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 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' 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 further 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/employee's objections. If an employee in a bargaining unit represented by a union makes a request for 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, 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, prior to the interview, request that they 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 military members. This is significant as 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, 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, 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. Military Service Members and Federal Employees. Military 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. Department of Defense 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 shall 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 in order 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' testimony, and to improve the accuracy and the quality of the report of investigation.

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. Prior to the start of an interview, explain to the witness that ODIG-AI policy is to record interviews. 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 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 they know 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 subjects or subjects, and their attorneys. This is intended to preserve the integrity of the investigation, and to protect confidentiality, the 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 that they are afforded the proper notifications of authorities and due process.

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

1. Introduction of the investigator and display of credentials;
2. Advise the witness that this is an administrative (not criminal) investigation;
3. Briefly state the purpose of the interview and explain why it is necessary to interview the witness;
4. 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;
5. Review and provide the witness with a copy of the Privacy Act Notification if they have not already been provided a copy; and
6. 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:

1. Date, time, and location of the interview;
2. Introduction of the investigators;
3. Identification of the allegations;
4. Statement that employee is a witness or subject;
5. Administer the oath;

6. Confirm that interview is recorded;
7. Confirm Privacy Act provided; and
8. Witness states name and title.

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

1. Ask if the witness wishes to provide any additional information;
2. Ask if the witness has any questions; and
3. Caution the witness not to discuss the testimony with anyone, except for their 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:

1. Ask specific questions to the witness to elicit the relevant information; or
2. 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.

5.6.6.3. Transcription Instructions Form. Investigators should exercise care and attention to detail in completing a transcription request form. Ensure that all names, locations, and acronyms are spelled out. Identify anything that a person outside DoD would not recognize.

5.6.6.4. Validating Transcripts. Investigators should validate transcripts by listening to the audio recording and comparing it to the transcript. This should be done for the key

statements cited in the report of investigation in support of the report's conclusions. It should also be done for "inaudibles" 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 phase, 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' title or position,how long they have been in that position, their responsibilities, and organizational and chain of command relationships.

5.7.2. Free Narrative/Indirect Questioning. During the free narrative/indirect questioning phase, the investigator should ask open-ended questions, asking the witness to talk about their knowledge of the events or actions under investigation in their 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 affords the opportunity for the witness to provide their 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. During direct questioning, the investigator should ask questions that get into 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 ask questions like "did you or did they" and "why did you or why did they?" During this phase of questioning, it is important to pin down the subject, require them to answer the questions and not let them evade or avoid the questions.

5.7.4. Cross-Examination. During the cross-examination phase, the investigator should address inconsistencies in the witness testimony, contradictions within the testimony, or conflicts between the witness testimony and the testimony of other witnesses. This is also the phase where the investigator should put the subject, or witness on notice if they believe that they are not being honest or truthful in their testimony. This is a good time to remind the witness of their responsibility to provide truthful testimony. This is a very critical phase of the interview and it is very 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 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 Service 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 for the purpose of facilitating the rendition of 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 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 caused the investigation to be conducted, 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 IG reports can have profound effects on the careers of DoD employees and on the public's trust and confidence in DoD officials and the Inspector General 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. There should be no errors in identifying people, places, dates, events, activities, or other basic factual information, nor should there be any errors in presenting witness testimony. Care should be exercised in 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 Inspector General organization. In order to avoid errors in writing, investigators must write from source documents, not from their memory.

6.2.2. Documentation. The findings of fact 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-CATS. Source documents for facts presented in the report should be maintained in a separate fact book folder in D-CATS. Source documents include: official records (personnel records, travel records, contract records, timesheets, etc.), testimonial evidence (pages from transcripts, reports of interviews, and/or e-mails, etc.), 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, or 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 IG reports should demonstrate to the reader that the allegations were treated seriously and that 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 IG.

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 where 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, 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 exculpatory, mitigating, or in dispute. Investigators' personal opinions are not to be included in DoD IG 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 field work. Factual information should be entered in to 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 roundtables throughout the fieldwork phase, resulting in a substantially written draft report upon the completion of fieldwork. The drafts should not include conclusions until the sufficient evidence has been gathered to form a conclusion based on the preponderance or clear and convincing standards.

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

6.3.1.1. Executive Summary/Introduction and Summary. The Executive 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 are:

6.1.1.1.1. 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.

6.1.1.1.2. 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

6.1.1.1.3. Recommendation Paragraph. We recommend that appropriate corrective action be taken with regard to 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.

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

6.3.1.3. Scope. This section is used to describe 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 that were interviewed, and any other special investigative techniques that were employed such as the use of subpoenas. This section is also used to address allegations that were not investigated within the scope of the investigation.

6.3.1.4. Findings and Analysis. This section is used to present the main findings of the report in a format comprised of standards, facts, discussion, and conclusions, organized under each of the issues/allegations addressed by the report. Note: In WRI reports the standards are presented in a separate section titled Statutory Authority which precedes the Findings and Analysis section.

6.3.1.5. 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.

6.3.1.6. Facts. This section is used to present the who, what, when, where, why, and how, relating to the issues/allegations under investigation. Present the factual information in detail to include 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 sub-headings 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.

Investigators must use the track changes and comment boxes containing hyperlinks to reference the source document; i.e. e-mail dated XX, witness testimony dated XX, page XX, contract dated XX, personnel document dated XX. NOTE: Citing source documents is critical in meeting professional standards and in performing the quality review process.

6.3.1.7. Discussion. In this section the investigator explains how they arrived at the conclusions. The language should plainly state that we have analyzed the evidence using the applicable standard of proof, *e.g.*, "preponderance of evidence" or "clear and convincing."

6.3.1.7.1. The Code of Federal Regulations 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. 5 C.F.R. 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. 5 C.F.R. Section 1209.4(d).

6.3.1.7.2. *Black's Law Dictionary* defines the standards as:

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

Clear and convincing evidence is that proof which 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. Start the discussion section by stating your conclusion in the first sentence, and then follow with information that walks the reader through how the evidence supports the conclusion.

Follow the elements of the applicable regulations and explain how the facts apply to those elements. Do not merely restate all of the facts in the discussion section. On the other hand, do not assume that anything, particularly your logic, is obvious. Be explicit in pointing out the specific facts that carried the most weight in reaching the conclusion.

It is especially important 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 Tentative Conclusion Letter (TCL) was issued, incorporate the subject's responses/arguments in the final report. Also address any additional fieldwork that was conducted subsequent to the TCL response, any new information discovered by the additional investigation, and how the new information impacted the tentative conclusions.

6.3.1.8. Conclusions. This section sets forth the conclusions for each of the allegations addressed under 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 is violated.

Example:

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

We conclude that 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 statute/reg).

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

Example:

We conclude that:

A. The senior official misused government resources in violation of (cite regulation).

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

6.3.1.9. 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, or command climate and/or morale issues.

6.3.1.10. Recommendations. This section is used to make recommendations for corrective actions.

6.3.1.10.1. In cases where misconduct is substantiated, recommend appropriate action. We do not recommend disciplinary action.

Example: We recommend the Secretary of the Service take appropriate action with respect to senior official/subject.

6.3.1.10.2. In cases where relief for the complainant is appropriate, recommend remedial action.

Example: We recommend that the Secretary of (the Service) take remedial action with respect to (complainant's name) unfavorable NCOER.

6.3.1.10.3. In cases where reimbursement to the government is appropriate, recommend reimbursement.

Example: We recommend that the Secretary of the Service direct General reimburse the government for his/her misuse of government resources for unofficial purposes.

6.3.1.10.4. In cases where systemic issues are identified, recommend specific corrective action.

Example: We recommend that the Secretary of the Service direct (put title of appropriate management official) establish/ strengthen/clarify policies and procedures governing official travel.

6.3.1.10.5. In cases where no corrective action is required, state that we make no recommendations.

Example: We make no recommendations in this matter.

6.3.1.11. 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. Quality Assurance Review Process

6.4.1 Review Process. All ODIG-AI final reports will undergo a quality review process in keeping with DoD Instruction 7600.1. The quality review process is to ensure that final reports meet the professional standards for quality, 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 DDIR/DIR review, and a legal review.

The process is a collective process that requires each member to accomplish their role with due diligence in order to produce reports that reflect the highest standards for quality and professionalism. All of those involved in producing reports must be mindful that reports of investigation are the product of the Office of the Inspector General. By CIGIE standards, investigators have a responsibility to be impartial, to remain objective and to be receptive to evidence that is exculpatory, 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 will 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 regarding 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 in D-CATS, check the revised report back in, and inform the SI that it is ready for the first supervisor review.

6.4.4.2. The SI will review the report by checking the report out in D-CATS using track changes, providing edits and comments, and checking the draft report back into D-CATS 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 have been made in the report.

6.4.4.3. Deputy Director/Director Review. Once the SI is satisfied with the draft report, they will inform the DDIR/DIR, who will then check out and review the report, make edits and comments in track changes, and check it back in for the investigator to make changes to the draft report as directed.

6.4.5 Editor Review. The editor will review the report prior to the Quality Assurance review. The editor will proofread the report to identify possible errors in grammar, syntax, spelling, typing errors, etc., and will ensure the proper template is used. The editor will check for compliance with the DoD Manual for Written Material and the AI Correspondence Manual, as well as consistency with the Government Printing Office Style Manual and the Federal Plain Language Guidelines. The editor will check out the final draft report in D-CATS and then check it back in for the investigator review.

6.4.6 Quality Assurance Review. As part of the ODIG-AI Quality Assurance Program, the ODIG-AI Program Analyst for Quality Assurance performs an independent review of the draft report of investigation. 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.

6.4.7 DIG-AI Review. Once a report has been approved by the Director, edited, and found to comply with CIGIE standards by the QA reviewer, it is ready to be forwarded for review by the DIG-AI. Investigators will send the package through the Special Assistant to DIG who will review all correspondence accompanying the report to ensure that it complies with OSD correspondence guidance. The DIG-AI then reviews the report and either returns the report to the SI to make edits as directed or forwards the report to OGC.

1. Electronic Routing and Transmittal Slip (OP-41) forwarding the package to DIG- AI with hyperlinks to TABs;

2. In cases where the report will be signed by the IG, include an Action Memo forwarding the report to the IG through DIG-AI with OGC edits;

3. Closure documents for DIG-AI or IG signature;

4. Closure documents to be signed by Director in reprisal cases;

5. Final copy of the ROI (under green cover if the report will be distributed outside the OIG); and

6. Previous IG correspondence regarding the investigation.

7. The final TAB in the package is the coordination page.

6.4.8 Office of General Counsel Review. Once the DIG-AI approves the draft, the report is routed to OGC for a review in D-CATS using the OP-41. The OGC assigned attorney will review the report for legal sufficiency, which includes ensuring the conclusions are supported by the evidence.

The investigator and the attorney from OGC will hold a roundtable discussion following the initial review by OGC in order to efficiently and effectively resolve any questions or concerns. Candid and clear communications will reduce the number of iterations in the draft review process and move more rapidly toward completing the investigation.

After the investigator has revised the draft report, it must be submitted to OGC for a final review and concurrence that it is legally sufficient prior to issuance.

6.5. Report Approval

6.5.1. Senior Official and Other High-Interest Investigations. Reports documenting senior official misconduct or other high-interest investigations may, in some cases, be forwarded to the PDIG and the IG for approval via e-mail by the DIG-AI. A hardcopy of the signed Action Memo along with any signature documents will be assigned a SCOUT number, uploaded into SCOUT, and assigned to the Executive Secretariat. SCOUT is the electronic tracking system that is used for reports and correspondence going to the PDIG or IG. Once in the IG front office, correspondence 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 DIGAI, Director, or directly to the investigator for further action.

6.5.2. Returned Reports. Investigators must keep their supervisors informed when a report is returned directly to them. Should substantive modification to the report be required, make sure the revisions are coordinated with the DIG-AI and the OGC. Pay particular attention to continuity in tracked changes in D-CATS. 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/Introduction and Summary section must be carried forward into closure memorandums and letters.

6.5.3. Distribution. Once the IG has approved the report by signing the closure memorandums and letters, the packet is returned to ODIG-AI for distribution. Procedures for distribution of documents, potential release of information, and disposition of files are discussed in Chapter 7, Case Closure.

6.6. Tentative Conclusion letters

In investigations where misconduct is substantiated, the ODIG-AI will provide the subject a tentative conclusion letter and an opportunity to comment on the tentative conclusion prior to issuing a report.

The tentative conclusion letter package includes a letter addressed to the subject of the investigation (or their attorney) and a copy of the draft ROI which has been redacted for source protection. The letter 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 FOUO and may not be copied or further released."

Tentative conclusion letters are either hand-carried or delivered by certified/express mail or e-mail. Subjects are generally afforded 2 weeks from the date of the letter to respond. Comments made by subjects or subjects will be considered, and further 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, due professional care, requires that the investigative report findings and accomplishments must be 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 has been approved, investigators should promptly accomplish case closure procedures.

Steps in the Case Closure Process

1. Prepare Closure Correspondence

2. Staffing Process
a. For Director Signature
b. For DIG-AI Signature
c. For IG signature or Director, OLAC signature

3. D-CATS Data Entry

4. Case File Preparation

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 report of investigation by 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 the 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-CATS as further described, below.

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:

1. E-mail forwarding the package to DIR WRI with hyperlinks to the appropriate closure correspondence.

2. A memorandum transmitting the final report of investigation to the appropriate officials. This memo provides a brief summary of the investigation findings.

3. The ROI.

Templates for ODIG-AI correspondence can be found AI SharePoint under the Template Library.

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 where it should be prepared for the Inspector General to sign when addressed to the Secretary or Deputy Secretary of Defense or Service Secretaries in high-interest cases. The staffing package must include:

1. Electronic routing slip forwarding the package to DIG-AI via e-mail with hyperlinks to the ROI and case closure documents.

2. 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.

3. A memorandum to the DoD management official transmitting the final ROI. This memo will provide a brief summary of the investigation findings.

4. The ROI.

5. TCL response as applicable.

6. Letter(s) to the subject or their attorney.

Templates for ODIG-AI correspondence can be found on the SharePoint AI SharePoint under the Template Library.

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-CATS must include:

1. Letter to the complainant transmitting the redacted ROI. This letter provides a brief summary of the investigation findings.

2. The redacted ROI.

3. Letters to appropriate officials.

Templates for ODIG-AI correspondence can be found on AI SharePoint in the Template Library.

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-CATs must include:

1. Electronic routing slip forwarding the package to DIG-AI via e-mail with hyperlinks to ROI and closure correspondence.

2. The letter to the subject of the investigation informing them that the investigation has been completed, and providing them 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 on AI SharePoint in the Template Library.

7.4 Congressional Inquiries

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

1. An Action Memorandum to the Director, OLAC providing a summary of the investigation findings.

2. 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 guidance below).

3. TAB B: A copy of the incoming Congressional.

4. TAB C: Previous correspondence (interim responses sent previously).

5. TAB D or last TAB is always reserved for coordination.

Templates for ODIG-AI correspondence can be found on AI SharePoint in the Template Library.

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. Do not mark the letter and the enclosure FOUO.

7.4.2.2. If the Member of Congress has written 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 FOUO 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 "FOR OFFICIAL USE ONLY." This letter may be released to [insert name of constituent], but other requests for this letter should be referred to the Department of Defense 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 un-redacted version of the report. If the report is FOUO, the closure letter will, in all likelihood, also contain FOUO 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 "FOR OFFICIAL USE ONLY." 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 Department of Defense 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 their responsibilities, to perform trend analysis, to measure accomplishments, to produce semi-annual 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 exculpatory 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 until 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 where 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 in order 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-CATS 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 1 – Incoming Complaint & Supplementals. Reserved for the incoming complaint and the component IGs notification. In addition, this folder is reserved for any supplemental information to the complaint.

7.6.1.2. Folder 2 – Intake Disposition. 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 3 – Investigative Planning. Reserved for the investigative planning documentation. The investigative planning folder is divided into the following subfolders:

A. Investigative Plans. 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 4 – Evidence. Reserved for all relevant evidence gathered while conducting the investigation. The evidence folder is divided into the following subfolders:

A. Testimony. Subfolder A will have a folder per every interviewee. This includes subjects, complainant, witnesses, and subject matter experts. Each testimony 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, Case Soft Suites files, and spreadsheets.

7.6.1.5. Folder 5 – 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 IGs ROI and attachments. The Reports folders is further divided into the following subfolders:

A. Fact Book. Reserved for the documents cited in the ROI. All of the documents in this folder should be in .pdf. Use the naming convention guidelines.

B. Tentative Conclusions Letter & Preliminary Report. Reserved for the Tentative Conclusions Letter, the red box, and the redacted version of the ROI.

C. Quality Assurance Review. Reserved for the completed quality assurance review checklist.

D. Internal Review Coordination. Reserved for action memos and transmittal letters used while conducting the internal review and approval process.

E. Investigator Checklist. (WRI only) Reserved for the Investigator Checklist completed by Component IG investigators and submitted with cases for oversight.

7.6.1.6. Folder 6 - Correspondence. Reserved for correspondence. This includes but is not limited to: correspondence from subject matter experts, all requests for information, and updates. This folder contains the following subfolders:

A. Investigator E-mails. Reserved e-mails relevant to the investigations. Examples include: RFIs and Coordination e-mails

B. 180-day Letter. (WRI only) Reserved for letters related to section 1034 & section 2409 only.

C. Congressionals. Reserved for acknowledgement, interim, and final letters to Members of Congress.

D. Closure Memos & Letters. Reserved for the closure memorandums and e-mails to the Component IGs, management officials, subjects or RMOsubjects, and complainants.

E. Corrective Actions & Remedies. Reserved for responses from the Service or organization regarding corrective action taken and remedies.

7.6.1.7. Folder 7 – Oversight Review. Reserved for the signed oversight closure document and the e-mail to 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.

7.6.1.8. Folder 8 – Internal Controls Checklist. Reserved for the Internal Controls Checklist.

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. Master file

and additional folders must be organized, properly annotated, and complete. The case file must be suitable for review by an outside audit or peer review team or oversight authority.

7.6.3.1. Documents to be Preserved in the Case File. It is the investigator's responsibility to ensure that all evidence used in support of the findings of the investigation is maintained in the final case file. It is also important to ensure that official documents are preserved in accordance with DoD Instruction 5015.2, "Records Management Program" which implements the National Archives and Records Administration guidelines. DoDI 5015.2 provides the following helpful guidance.

Official records are defined as "All books, papers, maps, photographs, machine- readable materials or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the U.S. Government 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 Government because of the informational value of the data in them." All official records will be included in D-CATS 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-CATS under Documents (Folder 6A).

The investigator will determine those e-mails that are considered official records and ensure that they are placed in D-CATS 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 IG personnel; and e-mails collected as evidence during the investigation.

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

Versions of the report of investigation located in D-CATS 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 but not limited to:

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 closed date.

7.7.5. Place in Closed Pending Follow-up Status. Status for closed substantiated cases where 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. The supervisor will initial-off on 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 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 are sent to FOIArequests@dodig.mil. Written requests are 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, to include 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 in order to control the release of information and to preserve the integrity of the ongoing investigation.

7.8.3. Requests within DoD for Official Purposes. ODIG-AI reports of investigation, including underlying documentation, may be released within 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 Fact Book, 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 OGC and carefully weighing the level of the disciplinary action being considered (i.e. 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 for 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 Director, OLAC. In most cases, a written request from the Member of Congress is required. Depending upon the nature of the request, a Member of Congress may be provided either unredacted material, or information redacted for public release (See Chapter 6, Case Closure).

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 IG 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 (television, radio, newspaper, news magazines, etc.) 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 CIGIE third general standard 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 Inspector General of the Department of Defense shall:

1. initiate, conduct, and supervise such audits and investigations in the Department of Defense (including the military departments) as the Inspector General considers appropriate; and

2. provide policy direction for audits and investigations relating to fraud, waste, and abuse, and program effectiveness.

8.1.2.2. DoD Directive 5505.06. The DoD IG shall:

1. 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. DoD Directive 7050.06. The DoD IG shall:

1. Review determinations by Component IGs that investigation of an allegation is not warranted. Notifies the DoD Component IG of approval or concerns.

2. Review the results of investigations into violations of restrictions and reprisals conducted by DoD Component IGs. Approves the results or ensures the DoD Component IG corrects inadequacies or initiates a follow-up investigation. Notifies DoD Component IG of approval.

8.1.2.4. Title 10 U.S.C. Section § 1034.

1. Subsection (c)(3)(E) provides that in the case of an investigation under subparagraph (D) within the Department of Defense, the results of the investigation shall be determined by, or approved by, the Inspector General of the Department of Defense.

2. Subsection (c)(5) provides that the Inspector General of the Department of Defense shall ensure that the Inspector General 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.

3. Subsection (d) provides that upon receiving an allegation under subsection (c), the Inspector General receiving the allegation shall 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 Inspector General 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, DoD IG will receive notification from the DoD Component IG of all reprisal allegations from DCIPS employees and 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 DoD IG expeditiously initiate or request the DoD Component with a statutory IG to initiate an investigation when 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(s) as well as the individual(s) alleged to have taken the reprisal action. DoD IG must also review and approve the results of investigations conducted by DoD Component statutory IGs or initiate a follow-up investigation to correct inadequacies or ensure that the DoD Component statutory IG corrects them, if the review determines that an investigation is inadequate.

Lastly, DoD IG must ensure the standards of proof applied in the investigation are a preponderance of 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

The WRI and ISO investigators perform oversight reviews pursuant to DoD IG authorities previously cited in this chapter. Investigators will perform reviews of 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 be addressed by an investigation. The WRI intake process is limited to analysis of the alleged protected communications/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 in scope to an interview of the complainant (if known) and a limited 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 which 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.

8.2.1.4. Review of Dismissals.

8.2.1.4.1. WRI. WRI investigators will review intakes from the Military Services 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."

a. Alleged PCs. Determine if the alleged PCs were properly identified and/or if there were any alleged PCs not addressed that should have been included in the intake. For PCs that were not properly identified, document so in writing and explain why they were not properly identified in the context of the statute/regulation. For PCs that were missed, document them and explain why they would or would not affect the outcome of the analysis. Also document the 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.

b. Alleged PAs. Determine if the alleged PAs were properly identified and/or if there were any alleged PAs not addressed that should have been included in the intake. For PAs that were not properly identified, document in writing why they were not properly identified in the context of the statute/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 the 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.

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

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

8.2.1.4.2. ISO. ISO investigators will review requests from Component IGs to dismiss allegations without conducting an investigation because they obtained information during the intake process indicating the allegation lacks credibility that, if proven, would constitute a violation of criminal law, including the Uniformed Code of Military Justice; a violation of a recognized standard; or misconduct of concern to the leadership of the DoD or the Secretary of Defense, especially when there is an element of unauthorized personal benefit to the senior official,

a family member, or an associate. The investigators, in coordination with ISO management, will determine to concur with the dismissal or to request that an investigation be conducted.

8.2.1.5. Investigations. WRI and ISO Investigators assigned to the oversight branch are responsible for performing reviews of reports of investigation submitted by the DoD Components. Investigators will complete an oversight worksheet for each investigation that they review. The worksheets will serve as a written record of the results of the investigator's 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.

8.2.2. Oversight Analysis. Investigators will perform a thorough review of the report of investigation or recommended closure without investigation. Investigators will review the reports for adherence to the CIGIE professional standards for due professional care.

For each of the CIGIE standards, investigators will document in writing whether the standard is met, whether there are deficiencies, and whether the deficiencies are significant such that they adversely impacted 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 impacted the outcome or adequacy of the investigation – do not approve the investigation for closure until 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 and/or the adequacy of the investigation.

8.2.3. Due Professional Care.

8.2.3.1. Independence.

- Was the investigator outside the immediate chain of command of the individual making the complaint and the individual(s) 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(s) 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.

8.2.3.2. 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.

8.2.3.3. Thoroughness.

- Was the complainant (if known) interviewed?
- Were the witnesses with knowledge of the matters under investigation interviewed?
- Was the subject interviewed?
- Were relevant documents obtained (includes e-mails)?
- Were all of the allegations addressed by the investigation?
- Were 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.

8.2.3.4. 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/or complete?
- If deficiencies exist, did they adversely affect the outcome or adequacy of the investigation? Explain why.

8.2.3.5. Timeliness.

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

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

8.2.4.1. If the investigator determines that the intake or investigation was conducted in a manner consistent with CIGIE standards in all aspects, 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.

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

8.2.4.3. In intakes or investigations that contain a significant deficiency or multiple deficiencies that adversely impacted the outcome or adequacy of the investigation, the investigator will request a roundtable discussion with the SI, the Branch Chief, and/or 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, then the investigator will prepare a letter for the Branch Chief signature that will return the case to the component for further investigation. In all situations, these actions will be documented in the AI case notes field in D-CATS. After the Component resubmits the intake or investigation for approval, the investigator will complete the oversight worksheet, ensuring that any remaining deficiencies are identified.

8.2.4.4. 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.) Reprisal and restriction cases investigated by the Service IGs under 10 U.S.C. § 1034 are not closed until the DoD IG has reviewed and approved the investigative work,

and the complainant has been notified of the results. Therefore, it is necessary to provide written notification to the Service IG after the oversight review process is complete.

8.2.4.5. 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 IG will provide a rating of the quality of individual cases in addition to valuable information on trends in systemic deficiencies in investigations within their Component. Closure forms should note discrepancies phrased in "teach and train" language to inform and provide educative guidance.

8.3. Documenting the Oversight Process

D-CATS 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-CATS 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 and/or established suspense dates.

8.4.1. Inventories. Oversight Teams will reconcile inventories of all open cases including investigations being conducted by the DoD Components, cases with DoD IG pending oversight review, and cases pending follow-up actions (notification of closure to complainant, command actions, and remedies). The reconciliation will verify that identifying data is correct for all cases, to include 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-CATS indicates have been open 150 days or longer. This notification shall remind the Component IG to submit the required 180-day notification letter if the case will not be closed within 180 days of filing, as established in DoDD 7050.06.

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