



March 2019

WHISTLEBLOWER PROTECTION

Analysis of DOD's Actions to Improve Case Timeliness and Safeguard Confidentiality

GAO Highlights

Highlights of [GAO-19-198](#), a report to congressional committees

Why GAO Did This Study

Safeguarding confidentiality to the maximum extent possible is essential for encouraging whistleblowers to report wrongdoing without fear of reprisal. In fiscal year 2018, DODIG received over 12,000 contacts from potential whistleblowers related to fraud, waste, abuse, employee misconduct, or other violations. The National Defense Authorization Act for Fiscal Year 2017 included a provision for GAO to review the integrity of DOD's whistleblower program. This report assesses the extent to which DODIG and the military service IGs (1) met and took steps to achieve key fiscal year 2018 timeliness and quality goals, (2) established processes to protect whistleblower confidentiality, and (3) are able to safeguard sensitive information necessary to handle whistleblower complaints. It also evaluates (4) the extent to which select cases involving certain senior DOD civilian officials met key requirements.

GAO assessed fiscal year 2018 IG performance data, surveyed all 108 DODIG employees who directly handle whistleblower complaints, reviewed IT security controls, and analyzed all 125 cases involving civilian DOD Presidential appointees with Senate confirmation dismissed by DODIG in fiscal years 2013-2017.

What GAO Recommends

GAO is making 12 recommendations, including that the IGs take additional actions to improve timeliness, develop additional procedures to protect whistleblower confidentiality, and take steps to further limit IG employee access to sensitive whistleblower information. DOD concurred with all of the recommendations.

View [GAO-19-198](#). For more information, contact Brenda S. Farrell at (202) 512-3604 or farrellb@gao.gov.

March 2019

WHISTLEBLOWER PROTECTION

Analysis of DOD's Actions to Improve Case Timeliness and Safeguard Confidentiality

What GAO Found

The Department of Defense Office of Inspector General (DODIG) and military service offices of inspector general (IG) met some but not all fiscal year 2018 timeliness and quality goals for handling whistleblower complaints. For example, DODIG met its goals related to referring complaints to the appropriate agency within a certain number of days. All IGs also generally met goals related to the quality of investigations. However, about 85 percent of DODIG reprisal and senior official misconduct investigations exceeded statutory and internal timeliness goals. Further, military service IGs did not meet most goals for handling cases within prescribed timeframes. For example, the service IGs averaged between 17 and 84 days to notify DODIG of their receipt of whistleblower reprisal allegations, exceeding the 10-day goal. The IGs have various initiatives underway to improve timeliness, such as a Naval IG program to reduce timeframes for initial credibility determinations. However, additional actions could provide a more targeted approach to improving performance against unmet timeliness goals—such as for senior official misconduct investigations—and better assure whistleblowers that their cases will be handled expeditiously.

DODIG and the military service IGs have policies to protect whistleblower confidentiality, but some gaps exist. For example, DODIG guidance for protecting whistleblowers who report internal DODIG misconduct does not specify key steps investigators should take to protect confidentiality, such as not identifying complainants during interviews with case subjects. Also, Air Force, Naval, and Marine Corps IG guidance does not specify when whistleblower identities can be disclosed without consent. Without updated guidance, the IGs cannot ensure the consistent implementation of confidentiality protections.

The IGs have taken steps to safeguard whistleblower information in their information technology (IT) systems and applications, such as by restricting access to case information through unique user permissions and by taking actions to follow DOD's IT risk management process. However, between 2016 and 2018, employees in all of the IGs have been able to access sensitive whistleblower information without a need to know. For example, DODIG determined that numerous restricted whistleblower records in its document repository were accessible to DODIG personnel without a need to know. Similarly, the Air Force IG's application did not restrict users from other DOD components from viewing Air Force IG case descriptions and complainant identities, while the Army IG's application and the Naval IG's system did not restrict personnel within those IGs from viewing allegations or investigations involving other personnel within those IGs. Additionally, employees in Marine Corps IG offices were able to see whistleblower cases assigned to other IG offices without a need to know. While some actions have been taken to address these issues, additional steps are needed to restrict access to case information in order to mitigate ongoing risks to whistleblower confidentiality.

DODIG generally met key documentation requirements for the 125 cases it dismissed without investigation involving civilian DOD Presidential appointees with Senate confirmation.

Contents

Letter		1
	Background	7
	IGs Met Some Timeliness and Many Quality Goals, but More Actions Could Improve Performance against Unmet Goals	15
	IGs Have Processes to Protect Whistleblower Confidentiality, but Some Gaps Exist	28
	IGs Are Able to Access Whistleblower Information to Perform Their Duties and Have Taken Some, but Not All, Required Steps to Safeguard It	36
	DODIG Generally Met Documentation Requirements in Senior Official Cases that GAO Reviewed and Reported Most Credible Allegations	50
	Conclusions	54
	Recommendations for Executive Action	55
	Agency Comments and Our Evaluation	57
Appendix I	Scope and Methodology	61
Appendix II	Additional Examples of DODIG Initiatives to Improve Timeliness	70
Appendix III	Characteristics of Closed Misconduct and Reprisal Cases Involving Civilian DOD Presidential Appointees with Senate Confirmation	72
Appendix IV	Survey of Select DODIG Employees	75
Appendix V	Comments from the Department of Defense	88
Appendix VI	GAO Contact and Staff Acknowledgments	100
Related GAO Products		101

Tables

Table 1: Whistleblower Protections for Department of Defense (DOD) Civilians, Contractors, and Military Servicemembers	9
Table 2: Extent to Which DODIG Met Fiscal Year 2018 Quality Goals for Investigations, Oversight Reviews, and Hotline Activities	21
Table 3: Examples of Recent DODIG and Military Service IG Initiatives to Improve Timeliness	26
Table 4: Examples of Confidentiality Protections Included in DODIG Policies and Procedures for Hotline Activities and Senior Official Misconduct and Reprisal Investigations	29
Table 5: Survey Responses on Confidentiality during Internal DODIG Processes	32
Table 6: Select Accessibility Issues Identified by DODIG from November 2017 through May 2018	44
Table 7: Employee Access Issues Involving Military Service IG Information Systems and Applications	46
Table 8: Distribution of Dismissed Cases Involving Civilian DOD Presidential Appointees with Senate Confirmation, Fiscal Years 2013-2017	66
Table 9: Organizations Contacted by GAO	68
Table 10: DODIG Dismissed Misconduct and Reprisal Cases Involving Civilian DOD Presidential Appointees with Senate Confirmation, by Number of Days to Close and Percentage, Fiscal Years 2013-2017	73

Figures

Figure 1: DOD Processes for Handling Whistleblower Complaints	12
Figure 2: Timeliness of Fiscal Year 2018 DODIG Senior Official Misconduct Cases Resolved During Intake, Reprisal Intakes, and Oversight Reviews	16
Figure 3: Timeliness of Fiscal Year 2018 DODIG Senior Official Misconduct and Reprisal Investigations	18
Figure 4: Timeliness of Fiscal Year 2018 DOD Hotline Referrals and Oversight of Completion Reports	19
Figure 5: Timeliness of Fiscal Year 2018 Military Service IG Senior Official Misconduct Notifications, Reprisal Notifications, and Reprisal Intake Reviews	23
Figure 6: Timeliness of Military Service IG Senior Official Misconduct and Reprisal Investigations	24

Figure 7: Change in Defense Case Activity Tracking System enterprise Projected Release Dates Between January and October 2018	43
Figure 8: Disposition of DODIG Closed Misconduct and Reprisal Cases Involving Civilian DOD Presidential Appointees with Senate Confirmation, Fiscal Years 2013–2017	51
Figure 9: DODIG Dismissed Misconduct and Reprisal Cases Involving Civilian DOD Presidential Appointees with Senate Confirmation, by Organizational Source, Fiscal Years 2013-2017	72
Figure 10: DODIG Closed Misconduct Case Allegations Involving Civilian DOD Presidential Appointees with Senate Confirmation, by Percentage, Fiscal Years 2013-2017	74

Abbreviations

CIGIE	Council of the Inspectors General on Integrity and Efficiency
D-CATS	Defense Case Activity Tracking System
D-CATSe	Defense Case Activity Tracking System enterprise
DOD	Department of Defense
DODIG	Department of Defense Office of Inspector General
IG	Office of Inspector General
IT	Information Technology
NIST	National Institute of Standards and Technology
PAS	Presidential appointee with Senate confirmation

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



March 7, 2019

The Honorable James M. Inhofe
Chairman
The Honorable Jack Reed
Ranking Member
Committee on Armed Services
United States Senate

The Honorable Adam Smith
Chairman
The Honorable Mac Thornberry
Ranking Member
Committee on Armed Services
House of Representatives

The integrity of the Department of Defense (DOD) whistleblower program is paramount to establishing a culture that encourages the reporting of potential fraud, waste, abuse, misconduct, and other complaints.¹ DOD offices of inspector general (IG)—including the DOD Office of Inspector General (DODIG) and the IGs of the Air Force, the Army, the Navy, and the Marine Corps—rely in part on whistleblowers to help improve government operations.² Because whistleblowers also risk reprisal—such as demotion, reassignment, and firing—IGs have a special responsibility to protect whistleblower identity to the greatest extent possible, and to investigate allegations in a timely, confidential, independent, and objective manner.³

¹ For the purposes of this report, the DOD whistleblower program is defined as the administrative investigative components of the Department of Defense Office of Inspector General and the military services' offices of inspector general that handle whistleblower allegations of misconduct and reprisal.

² The IGs of the Air Force, the Army, the Navy, and the Marine Corps are hereafter collectively referred to as military service IGs. We use the term "Naval IG" to refer to the Navy's Office of Inspector General, separate from the Marine Corps' Office of Inspector General.

³ Section 7(b) of the Inspector General Act of 1978, as amended, codified at 5 U.S.C., Appendix § 7(b), states that IGs shall not, after the receipt of a complaint or information from an employee, disclose the identity of the employee without the consent of the employee, unless the IG determines such disclosure is unavoidable during the course of the investigation. Pub. L. No. 95-452 (1978).

Congress and the former administration established a statutory and policy framework which defines responsibilities for investigating whistleblower allegations of DOD employee misconduct and for protecting DOD whistleblowers from reprisal. Under this framework, DODIG is responsible for investigating and overseeing the investigation of misconduct and reprisal allegations from certain DOD civilian employees, contractors, and military servicemembers, while the IGs of the military services are responsible for investigating and reporting allegations involving military servicemembers to DODIG. In recent years, members of Congress and the public have expressed concerns regarding the integrity of misconduct and reprisal investigations, including those involving senior DOD officials and DODIG employees. Further, DODIG has designated ensuring ethical conduct as a top management challenge for the department.⁴ In fiscal year 2018, DOD's Hotline received 12,470 complaints from potential whistleblowers.⁵

We have previously reported on DOD's whistleblower reprisal program. In February 2012, May 2015, and September 2017, we found that DOD faced challenges in overseeing its program and made 25 recommendations to help improve the timeliness, quality, independence, and performance measurement of military, civilian, and contractor investigations, among other things.⁶ DOD concurred with all of our

⁴ Department of Defense Office of Inspector General, *Top DOD Management Challenges, Fiscal Year 2018* (Nov. 20, 2017).

⁵ The DOD Hotline provides a confidential, reliable means to report violations of laws, rules, or regulations; mismanagement; gross waste of funds; abuse of authority; and serious security incidents that involve DOD.

⁶ GAO, *Whistleblower Protection: Actions Needed to Improve DOD's Military Whistleblower Reprisal Program*, [GAO-12-362](#) (Washington, D.C.: Feb. 22, 2012); *Whistleblower Protection: DOD Needs to Enhance Oversight of Military Whistleblower Reprisal Investigations*, [GAO-15-477](#) (Washington, D.C.: May 7, 2015); and *Whistleblower Protection: Opportunities Exist for DOD to Improve the Timeliness and Quality of Civilian and Contractor Reprisal Investigations*, [GAO-17-506](#) (Washington, D.C.: Sept. 29, 2017).

recommendations, and as of November 2018, has implemented 18 of them.⁷

Section 536 of the National Defense Authorization Act for Fiscal Year 2017 included a provision for us to review the integrity of DOD's whistleblower program.⁸ This report assesses the extent to which DODIG and the military service IGs (1) met and took steps to achieve key fiscal year 2018 timeliness and quality goals related to the handling of whistleblower complaints, (2) established processes to protect the confidentiality of whistleblowers, and (3) are able to access and safeguard classified and sensitive information necessary to handle whistleblower complaints. It also evaluates (4) the extent to which select misconduct and reprisal cases involving certain senior DOD civilian officials met key documentation and reporting requirements.⁹

For the first objective, we reviewed documentation and interviewed officials on DODIG and military service IG timeliness and quality goals, performance measures, and associated performance data for fiscal year 2018, along with ongoing and planned efforts to improve performance. We selected data from this period because they constituted the most complete and recent performance data available. Using the data, we assessed the extent to which DODIG and the military service IGs met

⁷ DOD has not yet fully addressed our 2015 recommendation to standardize the investigation process across the military services or our 2017 recommendations to assess the feasibility of collecting key workload data, and including such data in a future personnel requirements assessment; document threats to independence and incorporate such information into an evaluation of independence threats; establish and communicate a declination policy for nondiscretionary cases; revise its internal controls checklist to include all key case file documentation and investigative events; develop a process to fully implement requirements related to the oversight of defense intelligence component cases; and develop quality performance measures and enhance existing timeliness measures to reflect key attributes of successful performance measures.

⁸ See Pub. L. No. 114-328 §536, (2016) as amended by Pub. L. No. 115-91, §578 (2017).

⁹ Civilian Presidential appointees with Senate confirmation (PAS) include cabinet secretaries, agency heads, and undersecretary-level posts.

timeliness and quality goals defined by statute and internal IG policy.¹⁰ To identify factors affecting timeliness and quality, we interviewed IG officials and reviewed performance documentation. We also compared DODIG and military service IG efforts to improve timeliness and quality, both planned and completed, against Council of the Inspectors General on Integrity and Efficiency (CIGIE) standards for federal IGs¹¹ related to establishing performance plans with goals and performance measures, as well as *Standards for Internal Control in the Federal Government* related to assessing and improving performance.¹² We assessed the reliability of DODIG and military service IG data by administering questionnaires on data collection, storage, and compilation; interviewing cognizant officials; and reviewing case management system documentation and quality assurance procedures. We determined that these data were sufficiently reliable for the purpose of assessing the extent to which DODIG and military service IGs met fiscal year 2018 timeliness and quality performance goals related to the handling of whistleblower complaints.

For the second objective, we assessed DODIG and military service IG policies¹³ and procedures for handling whistleblower allegations against

¹⁰ Under 10 U.S.C. § 2409, as amended, investigations of contractor and subcontractor whistleblower reprisal complaints are required to be completed in 180 days or fewer, or DODIG must notify the complainant and obtain permission to extend the investigation for no more than an additional 180 days. Also, in military whistleblower reprisal cases under 10 U.S.C. § 1034 if, during the course of the investigation, the IG determines that it is not possible to submit the report of investigation to the Secretary of Defense and the secretary of the military department concerned within 180 days after the receipt of the allegation, the IG shall provide to the Secretary of Defense, the military department secretary, and the servicemember making the allegation a notice of a description of the current progress of the investigation and an estimate of the time remaining until the completion of the investigation and when the report will be submitted to the servicemember.

¹¹ See CIGIE, *Quality Standards for Federal Offices of Inspector General* (August 2012). CIGIE was statutorily established as an independent entity within the executive branch by the Inspector General Reform Act of 2008, Pub. L. No. 110-409 (2008) and codified at 5 U.S.C. Appendix. Primarily comprised of inspectors general, CIGIE's mission is to address integrity, economy, and effectiveness issues that transcend individual government agencies and develop policies, standards, and approaches to aid in the establishment of a well-trained and highly skilled workforce in the offices of IGs.

¹² GAO, *Standards for Internal Control in the Federal Government*, [GAO-14-704G](#) (Washington, D.C.: September 2014).

¹³ For example, see DOD Instruction 7050.01, *DOD Hotline Program* (Oct. 17, 2017); Air Force Instruction 90-301, *Inspector General Complaints Resolution* (Aug. 27, 2015); Army Assistance and Investigations Guide (January 2016); Secretary of the Navy Instruction 5370.5B, *DON Hotline Program* (Nov. 24, 2004); Secretary of the Navy Instruction 5430.57G, *Mission and Functions of the Naval Inspector General* (Dec. 29, 2005); and Marine Corps Order 5430.1A, *Marine Corps Inspector General Program* (Aug. 1, 2018).

DOD policy, CIGIE standards for federal IGs,¹⁴ and statutory protections related to safeguarding whistleblower confidentiality.¹⁵ We also reviewed the results of DODIG's quality assurance reviews of the Air Force (2017), Army (2018), and Naval (2016) IGs, and surveyed all 108 DODIG employees directly involved with the handling of whistleblower cases to ascertain whether, in their view, confidentiality processes are being implemented in accordance with guidance and standards, identify potential confidentiality issues, and to gather perceptions on the integrity of the internal process for reporting misconduct, among other things. The survey achieved an 80 percent response rate.

For the third objective, we reviewed documentation and interviewed officials on the extent to which DODIG and the military service IGs have developed, implemented, and assessed key information technology (IT) security controls, and authorized the IT systems and applications used to process, store, and transmit sensitive whistleblower information. These reviews were based on requirements and standards prescribed by DOD,¹⁶ the Office of Management and Budget,¹⁷ and the National Institute of Standards and Technology (NIST).¹⁸ We also reviewed documentation and interviewed cognizant officials on the development and implementation of the Defense Case Activity Tracking System enterprise (D-CATSe)—DOD's future system for managing whistleblower information across DODIG and the military service IGs. Separately, we reviewed data and information on the number and percentage of DODIG

¹⁴ See CIGIE *Quality Standards for Federal Offices of Inspector General* (August 2012) and *Quality Standards for Inspections* (Nov. 15, 2011).

¹⁵ See 5 U.S.C., Appendix § 7(b).

¹⁶ DOD Instruction 8510.01 *Risk Management Framework for DOD Information Technology* (Mar. 12, 2014) (Incorporating change 2, Jul. 28, 2017).

¹⁷ Office of Management and Budget, Circular No. A-130, *Managing Federal Information as a Strategic Resource*, (July 28, 2016).

¹⁸ See National Institute of Standards and Technology, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans*, Special Publication 800-53A, Revision 4 (December 2014); *Security and Privacy Controls for Federal Information Systems and Organizations*, Special Publication 800-53, Revision 4 (April 2013); and *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, SP 800-37, Revision 1 (February 2010). At the conclusion of our work, NIST published a new version of Special Publication 800-37. See National Institute of Standards and Technology, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, Special Publication 800-37, Revision 2 (December 2018).

and military service IG classified cases closed in fiscal year 2017, and the number and allocation of DODIG and military service IG staff possessing security clearances. We also reviewed the processes and procedures for storing and accessing classified information within DODIG and the military service IGs against DOD policy related to establishing controls to ensure access to classified information is limited to authorized persons.¹⁹

To determine the extent of substantiated and potential confidentiality violations and retaliatory investigations involving DODIG employees, we also obtained and analyzed fiscal years 2013–2018 data on known or perceived violations of confidentiality standards and retaliatory investigations from DODIG, the service IGs, the Office of Special Counsel,²⁰ and the CIGIE Integrity Committee.²¹ We selected the data covering this period of time because they were the most recent and reliable data available. We assessed the reliability of these data by administering questionnaires, interviewing cognizant officials, and reviewing the methods used to query IG case management systems for the data. We determined the data to be sufficiently reliable for the limited purpose of identifying potential confidentiality violations and retaliatory investigations.

For the fourth objective, we reviewed all 125 administrative misconduct and reprisal cases involving civilian DOD PAS subjects that were dismissed by DODIG in fiscal years 2013 through 2017. We chose to review cases from this period because they constituted the most recent and complete data in DODIG's case management system and because they would most accurately reflect the extent to which the majority of DODIG's cases included required documentation. To conduct this review, we developed and used a data collection instrument to capture information regarding general case characteristics and the presence of information and documentation required by DOD policies and CIGIE best practices. Core elements of this instrument were shared with DODIG

¹⁹ DOD Manual 5200.01, Vol.3, *DOD Information Security Program: Protection of Classified Information* (Feb. 24, 2012) (Incorporating change 2, Mar. 19, 2013).

²⁰ The Office of Special Counsel is an independent agency within the executive branch established under the Whistleblower Protection Act of 1989 to investigate whistleblower reprisal and other federal personnel action complaints.

²¹ The CIGIE Integrity Committee receives, reviews, and refers for investigation whistleblower complaints made against Inspectors General, designated staff members of an IG, and the Special Counsel and Deputy Special Counsel of the Office of Special Counsel.

officials to ensure alignment with the policies and practices in place when the cases were dismissed.

To help ensure the accuracy of the information we collected, two analysts reviewed each casefile and coded for the presence of required information using the data collection instrument. In the event that disagreement between the two analysts occurred, the analysts discussed and resolved the disagreement by identifying and reviewing supporting database information or documentation, and obtained the input of a third analyst, if necessary. We reviewed all cases dismissed during this period; as a result, the dismissed case data in this report do not have a sampling error.²² Separately, we also reviewed documentation from DODIG on civilian DOD PAS official allegations and investigation results reported to the Secretary of Defense and Congress since fiscal year 2013. Appendix I provides additional details about our scope and methodology.

We conducted this performance audit from October 2016 to March 2019 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

While this audit was initiated in October 2016, work was suspended from December 2016 until September 2017 due to other engagement work.

Background

DOD Personnel Misconduct

The Inspector General Act of 1978, as amended, provides that the IG may receive and investigate complaints or information from an employee concerning the possible existence of an activity constituting a violation of law, rules or regulations; gross mismanagement; gross waste of funds; abuse of authority; or a substantial and specific danger to public health or

²² During the course of our review, we removed five out-of-scope cases, reducing the number of cases reviewed from 130 to 125. Four cases were removed because the related allegations were investigated, and one case was removed because it was a record used to track an investigation occurring at a military service IG. See appendix I for more details on our file review methodology.

safety.²³ Violation of the law may also include a violation of a provision of criminal law, including the Uniform Code of Military Justice, which is codified in Title 10 of the United States Code.²⁴

Whistleblower Protections for DOD Personnel

Whistleblowers are protected from reprisal as a result of making a protected disclosure through various statutes, regulations, and presidential policy covering different DOD personnel groups. Table 1 summarizes the statutory and policy authorities covering DOD personnel, along with selected protected disclosures and prohibited personnel actions—which are two required elements of the test for determining whether there was reprisal against a complainant for whistleblowing. A protected disclosure is a disclosure of wrongdoing by a whistleblower to a party that is an eligible recipient of that disclosure, while prohibited personnel actions include those actions that are taken or threatened in response to a protected disclosure, such as termination, reassignment, or a significant change in duties, responsibilities, or working conditions.

²³ See 5 U.S.C. § 7(a), Appendix.

²⁴ Chapter 47 of Title 10, United States Code.

Table 1: Whistleblower Protections for Department of Defense (DOD) Civilians, Contractors, and Military Servicemembers

DOD personnel group	Authority	Selected protected disclosures	Selected prohibited personnel actions
Appropriated-fund civilians	5 U.S.C. §§ 2301 and 2302	Violation of any law, rule, or regulation, or mismanagement. Gross waste of funds. Abuse of authority. Substantial and specific danger to public health or safety.	Detail, transfer, or reassignment. Decision concerning pay, benefits, or awards. Any other significant change in duties, responsibilities, or working conditions.
Non-appropriated-fund instrumentality employees	10 U.S.C. § 1587	Violation of any law, rule, or regulation, or mismanagement. Gross waste of funds. Abuse of authority. Substantial and specific danger to public health or safety.	Disciplinary or corrective action. Any other significant change in duties or responsibilities inconsistent with the employee's salary or grade level.
Employee of a contractor, subcontractor, grantee, subgrantee, or personal services contractor	10 U.S.C. § 2409	Violations of any law, rule, or regulation related to a DOD contract or grant. Abuse of authority relating to a DOD contract or grant. Gross mismanagement of a DOD contract or grant.	Discharging, demoting, or otherwise discriminating against the employee.
Defense Civilian Intelligence Personnel System employees and employees with eligibility for access to classified information	Presidential Policy Directive (PPD) 19 50 U.S.C. § 3234	Violation of any law, rule, or regulation. Gross waste of funds. Abuse of authority. Substantial and specific danger to public health or safety. Gross mismanagement.	Termination. Reassignment. Demotion. Taking or withholding, or threatening to take or withhold, any action affecting an employee's eligibility for access to classified information.
Military servicemembers	10 U.S.C. § 1034	Violation of any law, rule, or regulation. Gross waste of funds. Abuse of authority. Substantial and specific danger to public health or safety. Gross mismanagement.	Taking or withholding, or threatening to take or withhold, a personnel action. Any other significant change in duties or responsibilities not commensurate with the servicemember's grade.

Source: GAO analysis of whistleblower statutes and Presidential Policy Directive 19. | GAO-19-198

DODIG and Military Service IG Roles and Responsibilities for Investigating Whistleblower Reprisal Complaints

DODIG and the military service IGs share responsibility for investigating misconduct and whistleblower reprisal complaints. Allegations of misconduct and other whistleblower complaints, including those involving senior officials, may be investigated by DODIG or a military service IG depending on the nature of the allegation or the DOD employees involved. Responsibilities for investigating whistleblower reprisal complaints differ according to DOD personnel type. Specifically, DODIG is responsible for investigating and overseeing DOD component investigations²⁵ of complaints alleging reprisal against certain DOD civilian employees,²⁶ and for investigating complaints alleging reprisal against DOD contractor, subcontractor, grantee, and subgrantee employees.²⁷ For complaints alleging reprisal against a military servicemember, DODIG has the authority to either investigate the complaint or refer it to a military service IG for action.²⁸ Most reprisal cases involving military servicemembers are investigated by the military services IGs, with DODIG oversight.

²⁵ Under the Intelligence Authorization Act for Fiscal Year 2014 and the Intelligence Authorization Act for Fiscal Year 2010, the defense intelligence component IGs—the IGs of the Defense Intelligence Agency, the National Geospatial-Intelligence Agency, the National Reconnaissance Office, and the National Security Agency—have independent statutory authority to conduct investigations of reprisal complaints brought by Defense Civilian Intelligence Personnel System employees. See Intelligence Authorization Act for Fiscal Year 2014, Pub. L. No. 113-126, § 412 (2(A)-(B)) (2014) and Intelligence Authorization Act for Fiscal Year 2010, Pub. L. No. 111-259, § 431(a) (2010) (codified at 5 U.S.C., Appendix §§ 8G and 12). The roles and responsibilities of DODIG and the component IGs are enumerated in Presidential Policy Directive-19 (PPD-19), *Protecting Whistleblowers with Access to Classified Information* (Oct. 10, 2012), and DOD Directive-Type Memorandum 13-008, *DoD Implementation of Presidential Policy Directive 19* (July 8, 2013) (Incorporating change 3, Feb. 9, 2016).

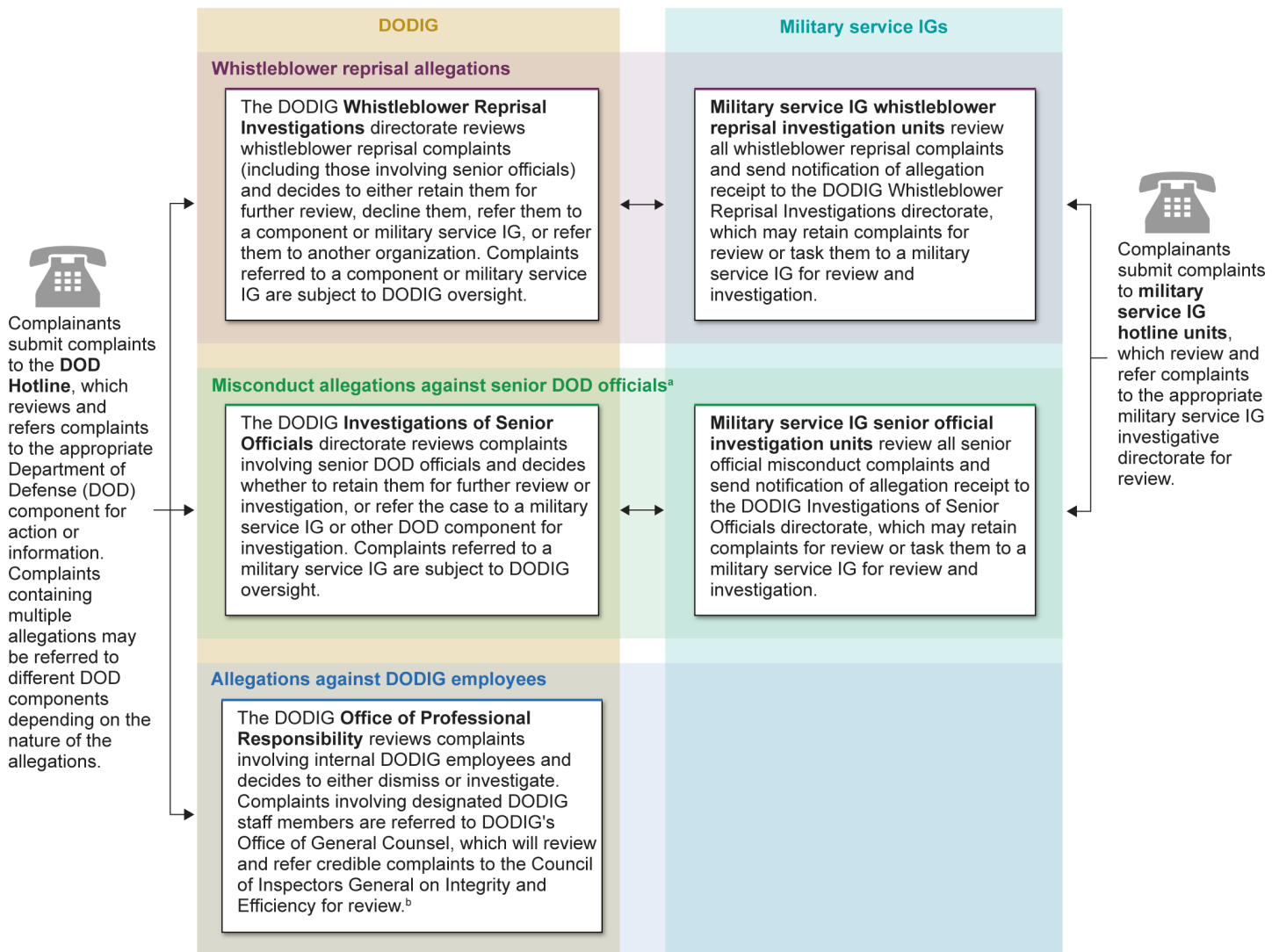
²⁶ DOD investigates all reprisal complaints from civilian *non-appropriated fund* employees under 10 U.S.C. § 1587. Under the Inspector General Act of 1978, as amended, DODIG may retain for investigation those civilian *appropriated-fund* complaints filed with DODIG that are of particular interest to DODIG, although the Office of Special Counsel has primary jurisdiction to investigate the majority of civilian whistleblower reprisal cases across the federal government, including those involving most DOD appropriated-fund civilians. The Office of Special Counsel is an independent agency established under the Whistleblower Protection Act of 1989 to investigate whistleblower reprisal and other prohibited personnel practices.

²⁷ Under 10 U.S.C. § 2409, DODIG is responsible for investigating all complaints of reprisal involving DOD contractor employees.

²⁸ Department of Defense Directive 7050.06, *Military Whistleblower Protection* (Apr. 17, 2015).

In order to carry out its responsibilities, DODIG has established several directorates to facilitate the handling and investigation of misconduct and reprisal complaints. Figure 1 provides a high-level depiction of the DODIG and military service IG processes for handling reprisal, senior official misconduct, and internal DODIG employee complaints, along with the basic roles of the DODIG directorates.

Figure 1: DOD Processes for Handling Whistleblower Complaints



Source: GAO analysis of Department of Defense Office of Inspector General (DODIG) and military service office of Inspector General (IG) information. | GAO-19-198

Note: This graphic depicts the interaction of DODIG and military service IGs in handling whistleblower reprisal and senior DOD official misconduct complaints. Military service IGs include the Air Force, Army, Navy, and Marine Corps IGs.

^aSenior officials are those current or former military personnel in the grade of O-7 and above, those selected for promotion to O-7, members or former members of the senior executive service and Defense Intelligence senior executive service, and current or former presidential appointees. The grade of O-7 is a Brigadier General in the Army, Air Force, and Marine Corps, and a Rear Admiral (lower half) in the Navy.

^bSection 11 (d)(4)(C) of title 5, U.S. Code, Appendix, requires IGs to annually submit to the CIGIE Integrity Committee a list of designated OIG staff members who report directly to an IG. In addition, each IG must designate any positions with significant responsibilities such that, in the judgment of the

IG and depending on the size and organization of the particular OIG, there is a heightened risk that an internal investigation of them would lack objectivity in fact or appearance. DODIG's most recent designated staff member memorandum was submitted in May 2018 and includes nine designated staff members.

Protecting Whistleblower Confidentiality

Whistleblowers confidentiality protections are codified in federal law. The Inspector General Act of 1978, as amended, restricts DODIG and military service IGs from disclosing a whistleblower's identity without the consent of the whistleblower unless the IG determines that such disclosure is unavoidable during the course of the investigation.²⁹ For example, if a complaint includes information that poses a personal or public safety concern, disclosing the identity of the complainant may be unavoidable. Additionally, the Privacy Act of 1974 prohibits the disclosure of records on any person to another agency without the consent of the person the record relates to, but allows for the disclosure of an employee's identity if the purpose is for routine use—that is, a use that is disclosed for a purpose compatible with the purpose for which it was collected.³⁰ For example, referring an allegation from an IG hotline to an appropriate investigative unit would be considered routine use.

Federal Law and Standards Establish Information Security Requirements to Protect Federal Systems

The Federal Information Security Modernization Act of 2014 is intended to provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations.³¹ The law requires each agency to develop, document, and implement an agency-wide information security program to provide risk-based protections for the information and information systems that support the operations and assets of the agency. The law also requires agencies to comply with NIST standards and the Office of Management and Budget requires agencies to comply with NIST guidelines for protecting federal IT systems.

Among other things, NIST defines how agencies should determine the security category of their information and information systems based on the potential impact or magnitude of harm that could occur should there be a loss in the confidentiality, integrity, or availability of the information or

²⁹ See 5 U.S.C., Appendix § 7(b).

³⁰ See 5 U.S.C. § 552a(b).

³¹ The Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283 (2014), partially superseded the Federal Information Security Management Act of 2002, enacted as title III, E-Government Act of 2002, Pub. L. No. 107-347 (2002).

information system. NIST also prescribes an array of activities associated with the selection, implementation, and assessment of IT security controls—and the authorization to operate federal IT systems and other products.

DOD Instruction 8510.01, *Risk Management Framework for DOD Information Technology*,³² established a risk management framework for DOD information technology that is consistent with the principles established in NIST Special Publication 800-37. This framework includes requirements and procedures for identifying, implementing, assessing, and managing security controls.

Council of the Inspectors General on Integrity and Efficiency (CIGIE) Standards

CIGIE's *Quality Standards for Investigations and Quality Standards for Federal Offices of Inspectors General* collectively provide a set of overarching principles that IGs should adhere to in conducting their operations. They also provide a framework for conducting high-quality investigations through the definition of general and qualitative standards.³³ General standards, among other things, address the qualifications of investigators, independence, and the concept of due professional care and confidentiality protections throughout the course of an investigation. Qualitative standards focus on the establishment of policies, procedures, and instructions for confidentially handling and processing complaints, along with investigative planning, execution, reporting, and information management.

The CIGIE Integrity Committee receives, reviews, and refers for investigation allegations of wrongdoing made against Inspectors General, designated staff members of an IG, and the Special Counsel and Deputy Special Counsel of the Office of Special Counsel.³⁴ Each Inspector General, including the DODIG, is required to submit a list of designated staff members to the CIGIE Integrity Committee Chairperson annually.

³² DOD Instruction 8510.01, *Risk Management Framework for DOD Information Technology* (Mar. 12, 2014) (Incorporating Change 2, Jul. 28, 2017).

³³ CIGIE, *Quality Standards for Investigations* (Nov. 15, 2011) and *Quality Standards for Federal Offices of Inspectors General* (August 2012).

³⁴ A staff member is an employee within a federal inspector general office who reports directly to an IG or is designated as a staff member in the annual submission to the CIGIE chairperson. See 5 U.S.C. Appendix § 11(d)(4)(B).

IGs Met Some Timeliness and Many Quality Goals, but More Actions Could Improve Performance against Unmet Goals

DODIG Met Some, but Not All, Fiscal Year 2018 Timeliness Goals

DODIG met some but not all internal timeliness goals for fiscal year 2018 related to the intake and referral of whistleblower allegations, as well as the oversight of DOD component investigations. DODIG also did not meet internal goals related to the timeliness of senior official misconduct investigations or internal and statutory goals related to the timeliness of reprisal investigations. Intake is the initial process to determine whether a complaint contains a prima facie allegation³⁵ of whistleblower reprisal or a credible allegation of misconduct by senior officials.³⁶ Oversight reviews are conducted by the DODIG whistleblower reprisal and senior official investigations directorates to ensure the quality of DOD component investigations.

DODIG officials cited several reasons for not meeting timeliness goals, including a backlog of cases and a lengthy report review process. Further, DODIG officials noted that the number of whistleblower reprisal cases increased from 1,013 to 2,002 (98 percent) over the past 5 years, while an internal DODIG fiscal year 2018 performance report cited other reasons for not meeting timeliness goals, including the assumption of responsibility for all sexual assault victim reprisal cases by the whistleblower reprisal investigations unit, the number of high-priority senior official cases concurrently open, and the increasing scope and complexity of investigations.

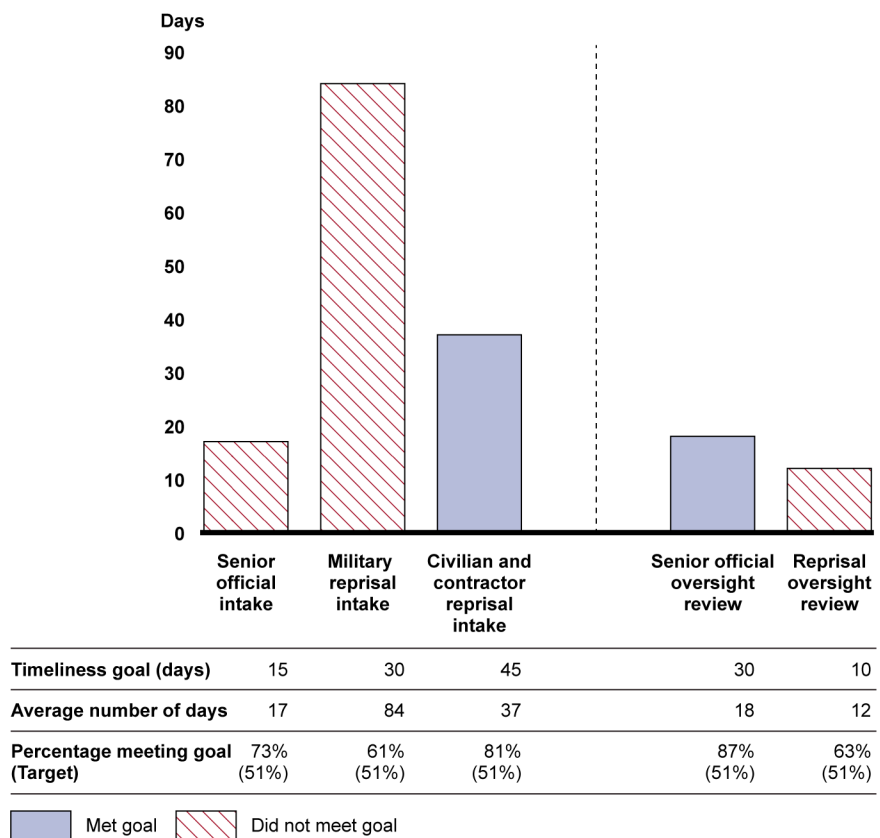
³⁵ Black's Law Dictionary, 10th ed. (2014), defines prima facie as "sufficient to establish a fact or raise a presumption unless disproved or rebutted, based on what seems to be true on first examination, even though it [may] later be proved to be untrue."

³⁶ Senior officials are those current or former military personnel in the grade of O-7 and above, those selected for promotion to O-7, members of the senior executive service and Defense Intelligence senior executive service, and presidential appointees. The grade of O-7 is a Brigadier General in the Army, the Air Force, and the Marine Corps, and a Rear Admiral (lower half) in the Navy.

Timeliness of DODIG Intake and Oversight Reviews

DODIG met its fiscal year 2018 timeliness goals for civilian and contractor case intakes and senior official misconduct oversight reviews goals, but did not meet goals related to the average days of senior official misconduct and military reprisal intakes, and the average days for reprisal oversight reviews (see figure 2). In fiscal year 2018, DODIG resolved and closed 631 senior official misconduct cases during the intake review process and it performed intake reviews for 1,032 whistleblower reprisal cases. It also conducted oversight reviews for 157 senior official misconduct cases and 995 reprisal cases.

Figure 2: Timeliness of Fiscal Year 2018 DODIG Senior Official Misconduct Cases Resolved During Intake, Reprisal Intakes, and Oversight Reviews



Source: GAO analysis of the Department of Defense Office of Inspector General (DODIG) data. | GAO-19-198

Note: Intake is the initial process to determine whether a complaint contains a prima facie allegation of whistleblower reprisal or credible allegation of misconduct by senior officials. Oversight reviews are conducted by the DODIG whistleblower reprisal and senior official investigations directorates to ensure the quality of DOD component investigation.

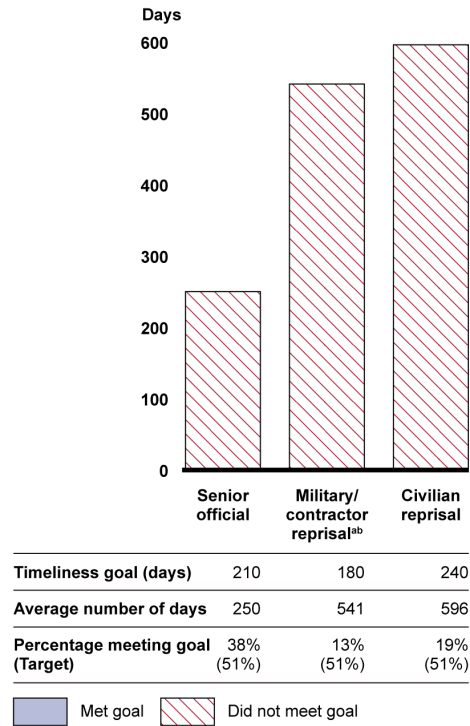
Timeliness of DODIG Senior
Official Misconduct and
Reprisal Investigations

By comparison, DODIG met its fiscal year 2017 targets related to the percentage of intakes and oversight reviews meeting timeliness goals, but it did not meet its goals for the average days of reprisal and senior official misconduct intakes.

DODIG did not meet internal or statutory timeliness goals related to the percentage or average days for senior official or reprisal investigations (see figure 3).³⁷ DODIG closed 73 investigations in fiscal year 2018, including 13 senior official misconduct cases and 60 military, contractor, and civilian reprisal cases. Overall, about 85 percent of all investigations did not meet the timeliness goal.

³⁷ The timeliness of investigations in fiscal year 2018 varied in comparison to fiscal year 2017. For example, the timeliness of senior official misconduct investigations improved from fiscal year 2017, during which none met the goal of 210 days or less, and the average days for investigations was 455 days. However, the average days to complete military and contractor reprisal investigations increased between fiscal years 2017 and 2018 from 394 days to 541 days, and the average days for civilian reprisal investigations also increased from 461 days to 596.

Figure 3: Timeliness of Fiscal Year 2018 DODIG Senior Official Misconduct and Reprisal Investigations



Source: GAO analysis of the Department of Defense Office of Inspector General (DODIG) data. | GAO-19-198

^aUnder 10 U.S.C. § 1034 if, during the course of the investigation, the IG determines that it is not possible to submit the report of investigation to the Secretary of Defense and the service Secretary within 180 days after the receipt of the allegation, the IG shall provide to the Secretary of Defense, the service Secretary concerned, and the servicemember making the allegation a notice of that determination including the reasons why the report may not be submitted within that time and an estimate of the time when the report will be submitted.

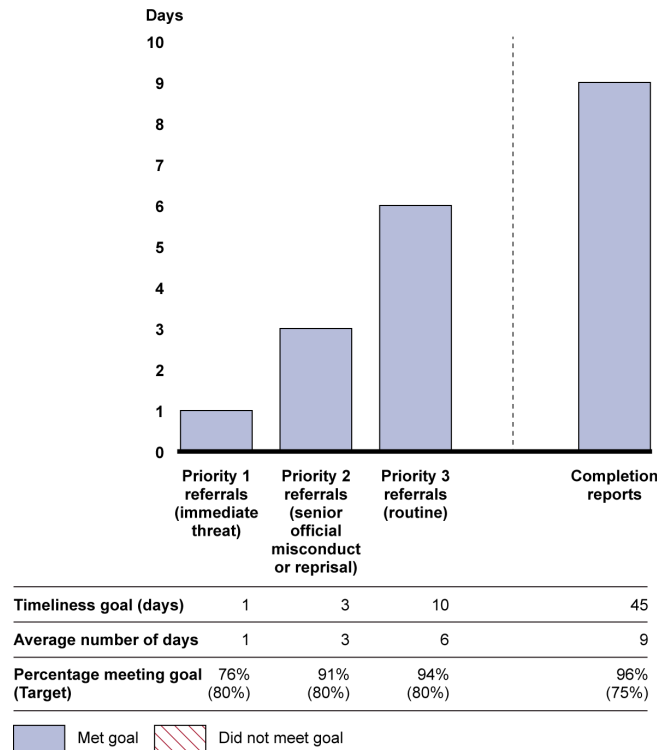
^bUnder 10 U.S.C. § 2409, as amended, investigations of contractor and subcontractor whistleblower reprisal complaints are required to be completed in 180 days or fewer, or DODIG must notify the complainant and obtain permission to extend the investigation.

DODIG similarly did not meet its investigation timeliness goals for senior official misconduct and reprisal investigations in fiscal year 2017. However, DODIG officials noted that the record closure of 60 reprisal investigations in fiscal year 2018 was a significant improvement over the 37 closed in fiscal year 2017, and DODIG data showed that the average age of closed and open investigations peaked in April 2018 and June 2018, respectively, and that both were lower as of January 1, 2019. Additionally, DODIG officials stated that they expected to eliminate the case backlog and reach a sustainable state of timeliness during fiscal year 2019.

Timeliness of DOD Hotline Referrals and Completion Report Reviews

In fiscal year 2018, the DOD Hotline referred 3,872 cases³⁸ to other entities for inquiry, and it performed oversight of 945 completion reports from DOD components.³⁹ As shown in figure 4, the DOD Hotline met its timeliness goals, except for the percentage of referrals meeting the goal for priority 1 complaints.

Figure 4: Timeliness of Fiscal Year 2018 DOD Hotline Referrals and Oversight of Completion Reports



Source: GAO analysis of the Department of Defense Office of Inspector General (DODIG) data. | GAO-19-198

Note: Completion reports are submitted by DOD components upon the completion of an investigation referred to the component by DOD Hotline.

³⁸ This number represents initial referrals. According to DODIG officials, the Hotline referred a total of 6,655 cases, with multiple referrals sometimes being made from a single Hotline complaint.

³⁹ A Hotline contact becomes a case when the Hotline opens and refers the case for action or information to a DODIG component, military service IG, DOD agency or field activity, or other agency outside of DOD. Hotline completion reports are completed by DOD components and submitted to DOD Hotline for oversight upon the completion of an investigation that was referred to the component by DOD Hotline.

Comparatively, in fiscal year 2017, the DOD Hotline did not meet timeliness goals for the average days or percentage of referrals, but did meet its goal for completion reports.

DODIG Generally Met Fiscal Year 2018 Internal Quality Goals

Quality goals can enhance the ability of organizations to provide reasonable assurance that they are exercising appropriate safeguards for federal programs, as demonstrated by our prior work.⁴⁰ DODIG generally met its fiscal year 2018 internal quality goals related to the thoroughness and completeness of senior official misconduct and whistleblower reprisal investigations, as well as the completeness and accuracy of information in DOD Hotline referrals.⁴¹ DODIG's internal quality goals for senior official misconduct and reprisal investigations pertain to the thoroughness of required case-file documentation and the integrity and completeness of data in its case management system. Criteria for assessing these goals include whether or not key documentation of the investigation—such as the incoming complaints and required notifications—are present in the proper folders in the case file, and whether start, end, or milestone dates have been recorded in the case management system. Criteria for assessing the completeness and accuracy of information in DOD Hotline referrals include checks on whether whistleblower consent is accurately documented and whether correspondence is addressed to the correct recipient. According to DOD Hotline officials, a weighted checklist was created in June 2018 that has greater focus on those criteria associated with protecting confidentiality.

In fiscal year 2018, DODIG reported that it conducted quality reviews for 59 whistleblower reprisal cases and 13 senior official misconduct cases. DODIG further reported conducting reviews related to the quality of DOD component investigations for 80 whistleblower reprisal cases and 80 senior official misconduct cases, while the Hotline reviewed the thoroughness of 1,954 referrals. As shown in table 2, DODIG either met or partially met its quality goals except for the data integrity and completeness goal for senior official investigations and the documentation goal for senior official oversight reviews.

⁴⁰ GAO, *DOD Personnel Clearances: Comprehensive Timeliness Reporting, Complete Clearance Documentation, and Quality Measures Are Needed to Further Improve the Clearance Process*, GAO-09-400 (Washington, D.C.: May 19, 2009).

⁴¹ Hotline manages the receipt and referral of DOD misconduct reports.

Table 2: Extent to Which DODIG Met Fiscal Year 2018 Quality Goals for Investigations, Oversight Reviews, and Hotline Activities

Activity goal	Target	Number/Percent of compliant assessment criteria	Percent of cases compliant	Goal met?
Reprisal investigations				
Thoroughness and documentation	≥ 81 percent	562/633 (89 percent)	100	Yes
Data integrity and completeness	≥ 81 percent	625/767 (81 percent)	78	Partially
Senior official investigations				
Thoroughness and documentation	≥ 81 percent	113/132 (86 percent)	100	Yes
Data integrity and completeness	≥ 81 percent	135/182 (74 percent)	69	No
Oversight reviews				
Thoroughness	≥ 81 percent	<i>Senior official</i> – 976/989 (99 percent)	100	Yes
		<i>Reprisal</i> – 1038/1119 (93 percent)	100	Yes
Documentation	≥ 81 percent	<i>Senior official</i> – 65/94 (69 percent)	66	No
		<i>Reprisal</i> – 89/102 (87 percent)	84	Yes
Hotline quality control				
Referral thoroughness	≥ 80 percent	1092/1131 (97 percent) ^d	88	Yes

Source: GAO analysis of Department of Defense Office of Inspector General (DODIG) information. | GAO-19-198

Note: A goal was partially met if only one of the targets for the percent of compliant assessment criteria or percent of cases compliant was met.

^aThe number of compliant criteria reflect only June through September 2018.

While we have reported DODIG’s performance against its quality measures, we recommended in September 2017 that DODIG develop quality performance measures and enhance then-existing timeliness measures to reflect key attributes of successful performance measures, and DODIG concurred. In November 2018, DODIG officials stated that DODIG is currently using the quality measures it had in place prior to fiscal year 2017, and noted that DODIG had developed DOD-wide quality performance measures for 2018 that measure the thoroughness of military service investigations. As a result, we continue to believe that our 2017 recommendation is valid in that DODIG’s performance measures should reflect key attributes of successful performance measures.

**Military Service IGs
Generally Did Not Meet
Fiscal Year 2018
Timeliness Goals**

Military service IGs generally did not meet internal and statutory timeliness goals related to the notification of receipt of allegations of reprisal and misconduct, intake reviews, or senior official misconduct and reprisal investigations.⁴²

Military service IG officials provided several reasons for not meeting the internal and statutory timeliness goals for notifications, intake reviews, and investigations. Specifically, officials cited an increasing number of complaints; the increasing complexity of complaints, such as those that include multiple allegations and subjects; staffing challenges, such as training related to the rotation of military staff; and the use of reservists, who only work part-time. In addition, a senior official from one military service IG noted that service IGs should be provided greater latitude in dismissing complaints without DODIG review and approval, such as for reprisal complaints where there is no protected communication or personnel action.

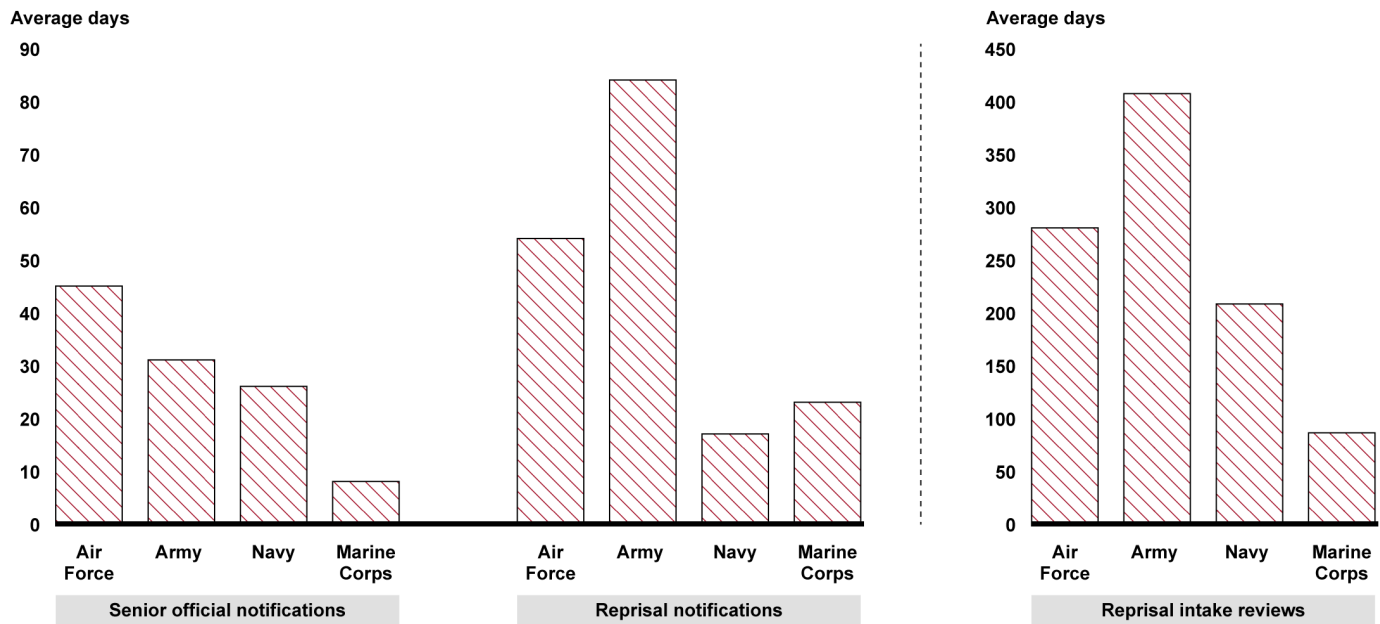
**Timeliness of Military Service
IG Notifications and Intake
Reviews**

The military service IGs did not meet fiscal year 2018 timeliness goals for notifying DODIG of allegation receipts, or conducting intake reviews for reprisal cases (see figure 5).⁴³ In fiscal year 2018, the military service IGs sent 141 senior official misconduct notifications and 876 reprisal notifications to DODIG, and performed 618 reprisal intake reviews.

⁴² Our assessment of military service IG timeliness is based on performance data provided by DODIG. As noted in figure 6, the Marine Corps did meet its senior official investigation timeliness goal.

⁴³ According to DODIG officials, DODIG does not assess the timeliness of military service IG intake reviews for senior official misconduct cases.

Figure 5: Timeliness of Fiscal Year 2018 Military Service IG Senior Official Misconduct Notifications, Reprisal Notifications, and Reprisal Intake Reviews



	Days		Average days			
	Timeliness goal	Met goal	Air Force	Army	Navy	Marine Corps
Senior official notifications	5	1	45	31	26	8
Reprisal notifications	10	0	54	84	17	23
Reprisal intake reviews	30	0	280	407	208	86

Met goal (solid blue) Did not meet goal (hatched red)

Source: GAO analysis of the Department of Defense Office of Inspector General (DODIG) data. | GAO-19-198

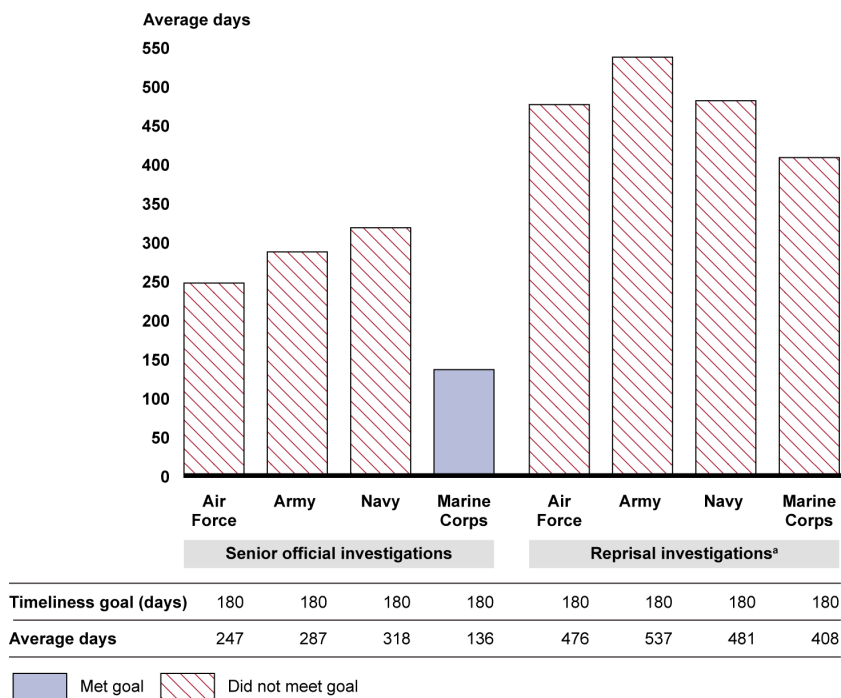
Note: DODIG data on reprisal intake reviews included two non-military reprisal cases, for which the timeliness goal is 45 days. However, DODIG data do not specify which military service IGs handled the cases.

Timeliness of Military Service IG Senior Official Misconduct and Reprisal Investigations

The military service IGs did not meet statutory or internal timeliness goals for senior official misconduct and whistleblower reprisal investigations, with exception of the Marine Corps IG—which met its goal for senior official misconduct investigations (see figure 6). In fiscal year 2018, the

military service IGs closed 424 investigations, including 347 reprisal investigations, and 77 senior official misconduct investigations.⁴⁴

Figure 6: Timeliness of Military Service IG Senior Official Misconduct and Reprisal Investigations



Source: GAO analysis of the Department of Defense Office of Inspector General (DODIG) data. | GAO-19-198

^aReprisal investigations include military reprisals and may include Presidential Policy Directive-19 reprisals, which have a 240-day goal. Under 10 U.S.C. § 1034 if, during the course of the investigation, the IG determines that it is not possible to submit the report of investigation to the Secretary of Defense and the service Secretary within 180 days after the receipt of the allegation, the IG shall provide to the Secretary of Defense, the service Secretary concerned, and the servicemember making the allegation a notice of that determination including the reasons why the report may not be submitted within that time, and an estimate of the time when the report will be submitted.

⁴⁴ DODIG data on military service IG reprisal intakes includes intake reviews for both military reprisal cases and an indeterminate number of Presidential Policy Directive-19 cases.

Military Service IGs Met DODIG and Internal Quality Goals for Investigations

Military service IGs met fiscal year 2018 quality goals established by DODIG related to the thoroughness of investigations conducted by the service IGs. Specifically, 89 percent of DODIG's thoroughness criteria were met in the 93 senior official misconduct investigations conducted by the military service IGs and other DOD components, exceeding the 81 percent goal established by DODIG.⁴⁵ Similarly, 85 percent of DODIG's thoroughness criteria were met in the 310 whistleblower reprisal investigations conducted by the military service IGs and other DOD components, exceeding the 81 percent goal established by DODIG. DODIG has established six criteria for assessing the thoroughness of senior official investigations, including whether all allegations were addressed, whether the complainant and subject were interviewed, and whether relevant documents were obtained. DODIG has seven criteria for assessing the thoroughness of reprisal investigations, including whether protected communications and personnel actions were identified, and whether the report of investigation was approved.

The Army, the Air Force, and the Marine Corps IGs also met internal quality goals for fiscal year 2018 related to the percentage of cases returned by DODIG for rework due to quality issues. Specifically, Army IG officials stated that they met their goal of having no more than 5 percent of the investigations they submitted to DODIG for review returned by DODIG due to quality issues, and Air Force IG officials stated that they met their goals of obtaining DODIG concurrence on all of the senior official investigations they submitted for review, and having no more than 5 percent of reprisal investigations returned for rework. Similarly, the Marine Corps IG achieved its goal of having no investigations returned for rework, according to a senior Marine Corps IG official. The Naval IG did not provide us with any internal quality goals.

Aside from the quality goals, DODIG also conducted quality assurance reviews for the Air Force (2017), Army (2018), and Naval (2016) IGs, in which the quality of a sample of case files was examined. The reviews concluded that the military service IGs reviewed were generally complying with internal regulations and CIGIE standards for quality. In addition, in accordance with recommendations made in the quality assurance reviews, each of the service IGs reviewed by DODIG has developed or plans to develop checklists to help ensure that all required

⁴⁵ Military service quality data presented in this report include data related to other DOD components, such as the defense intelligence components. DODIG data on the quality of military service IGs were available only in aggregate form, covering all DOD components.

documentation is present in their case files, according to service IG officials and documentation.

IGs Have Implemented and Planned Initiatives to Improve Timeliness, but Initiatives Do Not Target All Aspects of Timeliness

DODIG and the military service IGs have implemented and planned various initiatives to improve the timeliness of their processing of senior official misconduct and reprisal complaints. Table 3 shows examples of recent DODIG and military service IG initiatives.⁴⁶

Table 3: Examples of Recent DODIG and Military Service IG Initiatives to Improve Timeliness

DODIG	Military service IGs
DODIG has increased the number of staff in its whistleblower directorates from 114 to 147 full-time equivalents (about a 29 percent increase) since fiscal year 2016. ^a	The Air Force IG is developing a proposal to centralize its investigation function for reprisal cases instead of conducting these investigations at the local IG level. According to Air Force officials, centralizing this function would produce efficiencies by shortening the current review process for investigations and mitigating the effects of turnover at the local IG level.
DODIG is in the process of assessing its staff workload associated with different types of misconduct and reprisal cases, in response to our 2017 recommendation. This effort is intended to help inform its resource allocation. ^b	The Army IG reassigned internal staff to better assist with whistleblower reprisal caseload, and in November 2018 changed how reprisal case numbers are assigned to expedite the assignment process, according to an Army IG official.
DODIG and the military service IGs established a working group in August 2018 comprised of reprisal and senior official investigations representatives to identify efficiencies for military reprisal investigations, according to DODIG officials.	The Naval IG has implemented a pilot program which would meet the 30 day requirement to make a credibility determination, in part by eliminating prescribed preliminary analysis steps that went beyond the standard intake credibility determination.
DODIG implemented an alternative dispute resolution process in September 2017 to mediate reprisal complaints. According to DODIG officials, this process is a quicker alternative to an investigation, and it has provided significant relief to investigator caseloads by resolving many complaints that would have otherwise gone through the intake process, and potentially been investigated. ^c	The Marine Corps IG has hired an additional investigator and will hire a supervisory investigator, according to Marine Corps IG. These officials stated that they have also implemented procedures to more thoroughly intake and review complaints, along with an immediate credibility determination for all senior official complaints, thus speeding the timeline for doing so.

Source: GAO analysis of DODIG and military service IG information. | GAO-19-198

^aSpecifically, full-time equivalents increased in the senior official investigations unit from 29 to 33, the whistleblower reprisal investigations unit from 50 to 72, and the DOD Hotline from 35 to 42.

^bIn September 2017, we recommended that DODIG assess the feasibility of collecting additional workload data, such as the amount of direct and indirect labor hours associated with each case, and include such data in future personnel requirements assessments, as appropriate. See [GAO-17-506](#).

^cAccording to DODIG officials, the alternative dispute resolution unit reviews all contractor and subcontractor cases and non-appropriated fund civilian cases, as well as other select reprisal complaints.

⁴⁶ See appendix II for additional examples of timeliness improvements provided by DODIG.

While these initiatives are positive steps, given that the performance of some measures is far below the goals, additional efforts could be made to improve performance against unmet timeliness goals—including those pertaining to senior official misconduct investigations conducted by the military service IGs, military service IG notifications made to DODIG, and military service IG intake reviews for reprisal cases. Additionally, DODIG and some of the military service IGs do not agree on the timeframes prescribed by DOD policy for military service IGs to notify DODIG of the receipt of a complaint, thereby complicating achievement of these goals. For example, officials from the Air Force IG stated that they notify DODIG of the receipt of misconduct allegations only after making a credibility determination, instead of within the five working days of receipt prescribed by DOD policy for senior official allegations.⁴⁷ Similarly, Marine Corps IG officials stated that senior official allegations should be reported to DODIG within five days of a credibility determination.

Standards for Internal Control in the Federal Government state that management should complete and document corrective actions to remediate internal control deficiencies in a timely manner.⁴⁸ Expanding initiatives to target unmet goals related to military service senior official investigations, notifications, and intakes could provide DODIG and the military service IGs a more comprehensive approach to improving timeliness and better position the IGs to improve upon the timeliness goals prescribed by DOD policy. In addition, resolving disagreements related to notification timeliness could improve the military service IGs' ability to achieve those goals. Further, additional initiatives could provide greater assurance to potential whistleblowers that their cases will be handled expeditiously.

⁴⁷ See Department of Defense Directive 5505.06, *Investigations of Allegations Against Senior DOD Officials* (June 6, 2013) and Department of Defense Directive 7050.06, *Military Whistleblower Protections* (Apr. 17, 2015).

⁴⁸ [GAO-14-704G](#).

IGs Have Processes to Protect Whistleblower Confidentiality, but Some Gaps Exist

DODIG Has Policies and Procedures to Protect DOD Whistleblower Confidentiality

DODIG has established policies and procedures to implement key statutory requirements⁴⁹ and CIGIE standards⁵⁰ for protecting the confidentiality of whistleblowers from the receipt of a whistleblower complaint through its investigation. The Inspector General Act of 1978, as amended, states that the Inspectors General shall not, without consent from the employee, disclose the identity of an employee who reports misconduct or provides information, unless the Inspector General determines that such disclosure is unavoidable during the course of the investigation. Further, CIGIE's *Quality Standards for Investigations* states that policies, procedures and instructions for handling and processing complaints should be in place to ensure that basic information is recorded, held confidential, and tracked to final resolution. Table 4 shows examples of key confidentiality protections included in DOD Hotline and senior official misconduct and whistleblower reprisal investigation policies.

⁴⁹ Inspector General Act of 1978 (as amended) (codified at 5 U.S.C., Appendix § 7(b)) and 5 U.S.C. § 552a.

⁵⁰ CIGIE, *Quality Standards for Federal Offices of Inspector General* (August 2012) and *Quality Standards for Investigations* (Nov.15 2011).

Table 4: Examples of Confidentiality Protections Included in DODIG Policies and Procedures for Hotline Activities and Senior Official Misconduct and Reprisal Investigations

DOD Hotline	<p>DOD Hotline staff are required to obtain verbal or written consent from whistleblowers to disclose their identity outside of DOD Hotline on a need-to-know basis. The whistleblower's decision to consent or not must be documented in the case record.</p> <p>Select complaints—such as those involving DODIG employees—are to be restricted in the DOD Hotline's case management system.</p> <p>Cases involving whistleblowers that do not consent to the release of their identity are to undergo a quality control review prior to referral to ensure the complaints are properly redacted.</p> <p>Release of reports of investigation pursuant to the Freedom of Information Act^a or DODIG's proactive release policy are redacted and reviewed prior to release by either the DODIG Freedom of Information Act Office or the DODIG Office of General Counsel, as appropriate.^b</p>
Senior official misconduct and reprisal investigations	<p>Investigators are to exercise caution when contacting whistleblowers and conducting whistleblower clarification interviews, especially in their workplace, so as not to compromise identity.</p> <p>Investigators are to inform witnesses that DODIG is committed to protecting their confidentiality to the maximum extent possible within the law, and obtain witness acknowledgement of recording interviews at the outset of any interview.</p> <p>Information shared with subjects at the conclusion of an investigation, such as a copy of the draft record of investigation, is to be redacted in order to protect the whistleblower and other sources of information.</p> <p>Reports of investigation and underlying documentation supporting the reports, such as witness information, may be redacted to protect confidentiality, should circumstances warrant.</p>

Source: GAO analysis of Department of Defense Office of Inspector General (DODIG) policies and procedures. | GAO-19-198

^aSee 5 U.S.C. § 552. The Freedom of Information Act requires federal agencies to provide the public with access to certain government information on the basis of the principles of openness and accessibility in government.

^bDODIG's proactive release policy aims to release in a timely fashion, and to the extent possible, final reports and other records and information related to DODIG's performance of its statutory duties to Congress, other government agencies, the news media, and the public.

DODIG officials stated that they routinely emphasize the importance of protecting whistleblower confidentiality and that confidentiality policies and procedures are addressed through internal training, staff meetings, and on-the-job instruction. Further, 69 of 86 (80 percent) DODIG respondents to our survey reported believing that the guidance they received on protecting confidentiality is sufficient to maintain the confidentiality of individuals involved in IG investigations, citing many of the processes identified in table 4 above as examples of guidance they have received.⁵¹

⁵¹ Notably, 72 survey respondents (84 percent) also stated that they will seek direction from a supervisor for guidance on how to maintain the confidentiality of all individuals involved in the records they handle.

DODIG Guidance for Protecting the Confidentiality of Whistleblowers Who Report Internal DODIG Misconduct Lacks Sufficient Detail

The DODIG Office of Professional Responsibility's investigations manual⁵² on handling misconduct complaints against internal DODIG employees requires that complainant information be strictly controlled in order to protect the integrity of the investigative process and to avoid potential harm to the privacy and reputation of the employee.⁵³ This guidance also includes some steps to protect whistleblower information such as redacting substantiated reports of investigation to be provided to investigation subjects. As previously noted, DOD Hotline guidance also includes steps to protect the confidentiality of internal DODIG whistleblowers. However, the Office of Professional Responsibility guidance does not include several key steps and procedures that some DODIG officials reported taking to protect whistleblower confidentiality, such as excluding complainant information from notifications sent to subjects and not identifying complainants during interviews with case subjects. In addition, DODIG's Office of General Counsel does not have documented procedures for controlling access to cases involving designated DODIG staff members subject to review by the CIGIE Integrity Committee.⁵⁴ DODIG designated staff members include the Principal Deputy Inspector General, Deputy Inspectors General, General Counsel, and Senior Advisor to the Inspector General, among other staff members.

Guidance on handling complaints alleging internal DODIG misconduct is also outdated and does not reflect recent organizational changes. In particular, the Office of Professional Responsibility's investigations manual does not reflect its updated roles and responsibilities since splitting from the Quality Assurance and Standards directorate in October 2016, and certain chapters do not recognize that it now reports directly to

⁵² The investigations manual consists of seven chapters updated at different points between July 2009 and July 2013.

⁵³ The DODIG Office of Professional Responsibility reported receiving 415 complaints from fiscal year 2013 through fiscal year 2018, of which 84 complaints were investigated (50 were substantiated) and 199 were provided to other DODIG components for further consideration and action, as appropriate. Of the 415 complaints received, 123 (about 30 percent) were referred to the office from the DOD Hotline.

⁵⁴ Section 11 (d)(4)(C) of 5 U.S.C., Appendix, requires IGs to annually submit to the CIGIE Integrity Committee a list of designated OIG staff members who report directly to an IG. In addition, each IG must designate any positions with significant responsibilities such that, in the judgment of the IG and depending on the size and organization of the particular OIG, there is a heightened risk that an internal investigation of them would lack objectivity in fact or appearance. DODIG's most recent designated staff member memorandum was submitted in May 2018 and includes nine designated staff members.

the Inspector General.⁵⁵ Further, sections of the manual have been revised at different points in time and do not align with the office's current functions. For example, the section covering the office's organization, mission, and authorities has not been updated since July 2009. Similarly, the section detailing investigation policies and procedures has not been updated since November 2012.

Some of the DODIG employees we surveyed reported concern that DODIG's process for reporting employee misconduct and resolving internal complaints may not protect whistleblower confidentiality. For example, 14 (16 percent) survey respondents reported believing that DODIG's internal process for reporting misconduct did not protect DODIG employee confidentiality or only protected it slightly. Also, 36 (42 percent) survey respondents reported not knowing whether or not DODIG's internal process for reporting misconduct protects confidentiality, and 36 (42 percent) reported believing that it protects confidentiality somewhat or very well.⁵⁶ Additionally, 14 of 86 (16 percent) and 9 of 86 (10 percent)⁵⁷ employees surveyed reported having considered but ultimately choosing not to resolve an issue through the Office of the Ombuds—which may receive some internal misconduct complaints—or report misconduct through DODIG's internal process on or after October 1, 2016,

⁵⁵ Prior to October 2016, the Quality Assurance and Standards directorate was responsible for investigating internal DODIG employee misconduct and performing quality inspections and audits of DODIG components. According to DODIG officials, separating the two functions was intended to make the Office of Professional Responsibility a separate and independent office.

⁵⁶ According to the 2018 Federal Employee Viewpoint Survey, about 16 percent of DOD survey respondents and 15 percent of DODIG respondents disagreed or strongly disagreed with their ability to disclose a suspected violation of law, rule, or regulation without fear of reprisal, and about 16 percent of DOD respondents and 13 percent of DODIG respondents neither agreed nor disagreed. See *United States Office of Personnel Management, 2018 Federal Employee Viewpoint Survey: Report by Agency*. The Office of Personnel Management administers the survey annually to measure employee perceptions of conditions that contribute to their organization's success.

⁵⁷ In commenting on a draft of this report, DODIG officials expressed concern that we were not reporting the more substantial number of respondents that responded to our survey questions positively. However, the number of employees surveyed that reported considering but ultimately choosing to not resolve an issue through the Office of the Ombuds or report misconduct through DODIG's internal process because they feared their confidentiality could be compromised represent subsets of those employees who responded that they chose to not do so for one reason or another (e.g., concern about length of process, issue resolved through another avenue). As a result, it cannot be reported that 84 percent or 90 percent of respondents did not fear their confidentiality would be compromised. See appendix IV for additional information on our survey.

respectively, because they feared that their confidentiality could be compromised.⁵⁸ Table 5 shows the distribution of these responses.

Table 5: Survey Responses on Confidentiality during Internal DODIG Processes

Extent that respondents believed DODIG's internal process for reporting misconduct protected the confidentiality of DODIG employees.		
Not at all/slightly	Somewhat/very well	I don't know
14	36	36
Extent that respondents who considered reaching out to the DODIG Office of Ombuds, but ultimately chose not to, indicated that fear that confidentiality would be compromised influenced their decision to not reach out.^a		
Slightly	Somewhat	Very much
1	3	10
Extent that respondents who considered reporting misconduct against a DODIG employee through DODIG's internal process on or after October 1, 2016, but ultimately chose not to, indicated that fear that confidentiality could be compromised influenced their decision not to report through that process.^b		
Slightly	Somewhat	Very much
0	1	8

Source: GAO survey of Department of Defense Office of Inspector General (DODIG) employees. | GAO-19-198

^{a,b}These questions included response options of "not at all" and "don't recall," neither of which was selected by survey respondents.

Survey respondents identified some concerns related to the confidentiality, objectivity, and independence of DODIG's internal process for reporting misconduct and suggested some related improvements.⁵⁹ For example, although it has separated from the Quality Assurance and Standards directorate, the Office of Professional Responsibility continues to share office space with the directorate and hold complainant and

⁵⁸ The Office of the Ombuds functions as an independent, impartial, and confidential resource for employees to resolve conflict among DODIG employees. During the course of performing its duties, the Office of Ombuds may receive allegations of DODIG employee misconduct, which are to be forwarded to the Office of Professional Responsibility for review. According to DODIG guidance, the Ombuds shall not disclose the identity of any individual contacting the Office of the Ombuds or reveal information provided in confidence that could lead to the identification of any individual contacting the office without the individual's explicit permission. DODIG employees may consent to the disclosure of their identity when they elect to participate in resolution with management, according to DODIG officials.

⁵⁹ We presented these examples because they aligned with other information obtained during our review. For example, a DODIG employee that we interviewed similarly noted that holding complainant and witness interviews in the shared space was problematic. These examples were provided by one or more different respondents.

witness interviews in the shared space.⁶⁰ Also, it was suggested that an online form could be used so that internal complaints are routed directly to the Office of Professional Responsibility instead of through the DOD Hotline. DODIG officials told us that there are record-keeping and performance measure-related bases for continuing to use the DOD Hotline to receive complaints of internal misconduct, but that they would carefully evaluate the suggestion.

CIGIE Quality Standards for Federal Offices of Inspector General state that IGs should establish and follow policies and procedures for receiving and reviewing allegations and ensure that whistleblower identities are not disclosed without consent, unless the IG determines that such disclosure is unavoidable during the course of the investigation. *CIGIE Quality Standards for Investigations* also state that policies and procedures should be revised regularly to align with current laws and regulations. DODIG officials told us in November 2018 that the Office of Professional Responsibility investigations manual is in the process of being updated but were unable to provide a timetable for the completion of these updates, and stated that all of the provisions—including the confidentiality protections—are subject to changes and updates. In addition, in January 2019 DODIG officials noted, after discussion with GAO, that they intended to implement guidance for making referrals to the CIGIE Integrity Committee. Until DODIG develops guidance that incorporates procedures to protect confidentiality and documents how to maintain whistleblower confidentiality throughout the CIGIE referral process, it will lack reasonable assurance that its process for investigating internal misconduct allegations can fully protect the confidentiality of whistleblowers.

⁶⁰ According to DODIG officials, Office of Professional Responsibility personnel take reasonable and prudent measures to protect confidentiality, including by using private offices and a separate conference room for meeting with complainants, witnesses, and subjects. DODIG officials also stated that Office of Professional Responsibility personnel use white noise machines for conversations with complainants and others, and noted that all DODIG personnel must have personal swipe access or request entrance to every suite in DODIG, so the presence of an “unknown” or unfamiliar person in any suite, including the Office of Professional Responsibility, is neither significant nor noteworthy. Additionally DODIG officials stated that it was not clear whether separating the Office of Professional Responsibility would improve confidentiality, and that DODIG employees could observe how walks into a separate office and have more certainty that the employee was going to see the Office of Professional Responsibility rather than the Quality Assurance and Standards directorate.

Military Service IGs Have Guidance for Protecting Whistleblower Confidentiality, but It is Not Comprehensive

Military service IG guidance identifies confidentiality as a core tenet of handling and investigating whistleblower complaints.⁶¹ For example, military service IG guidance states that consent should generally be obtained from complainants before each military service IG can share a complainant's identity with officials who will investigate the allegations, and provides that complaints may be redacted or summarized to omit personally identifiable information—such as when consent is not given or for other purposes. In addition, military service IG guidance state that a complainant's identity may only be disclosed without consent when an authorized official has determined that such disclosure is unavoidable in order to investigate an allegation.

Aside from these shared provisions, each of the military service IGs' guidance includes additional precautions aimed at protecting whistleblower confidentiality. For example, Air Force Instruction 90-301 instructs Hotline personnel to coordinate communication between the complainant and investigator if a complainant does not give consent to disclose his or her identity. In addition, Army and Marine Corps IG guidance stipulate that whistleblowers will be notified if it becomes necessary to disclose their identity without their consent, and Naval IG guidance requires investigators to inform complainants that although the use of their testimony may be necessary under administrative action procedures, their identity will be released as a witness, not a complainant, to safeguard their identity.

While all military service IGs acknowledge the need to preserve confidentiality, we found gaps in confidentiality protections in Air Force, Naval, and Marine Corps IG guidance, but not Army IG guidance. For example, we found that Air Force, Naval, and Marine Corps IG guidance did not include requirements outlined in DOD Instruction 7050.01 related to the specific conditions under which information disclosures may be made without complainant consent.⁶² According to DOD Instruction

⁶¹ Air Force Instruction 90-301, *Inspector General Complaints Resolution* (Aug. 27, 2015); Army Regulation 20-1, *Inspector General Activities and Procedures* (July 3, 2012, revised on Feb. 13, 2018); Secretary of the Navy Instruction 5370.5B, *DON Hotline Program*, (Nov. 24, 2004); Department of the Navy, *Hotline Program Standard Operating Procedure*, (November 2016); Inspector General of the Marine Corps, *Marine Corps Inspectors General Program Concepts and Systems Guide* (August 2009); Inspector General of the Marine Corps, *Marine Corps Inspector General Program Investigations Guide* (August 2009).

⁶² DOD Instruction 7050.01, *DOD Hotline Program* (Oct. 17, 2017).

7050.01, these include circumstances when a complainant has made it known outside IG channels that he or she submitted the complaint, there is an emergency situation or health or safety issue, or the allegation is being transferred outside of DOD to another IG. Air Force, Naval, and Marine Corps IG guidance predate DOD Instruction 7050.01, updated in October 2017, and reference an older instruction that omits this disclosure guidance.⁶³

Additionally, DODIG's 2016 and 2017 quality assurance reviews of the Naval IG and Air Force IG concluded that confidentiality protections could be improved. Specifically, DODIG found that the Air Force IG did not have written procedures for handling and restricting IG employee access to complaints against individuals with access to the Air Force IG's whistleblower database, including both IG employees and contractors that support the database. In addition, DODIG found that the Naval IG Hotline program instruction needed to be updated and that it did not have a hotline standard operating procedure with guidance to redact complainant identities before releasing investigation reports to installation commanders or other military officials.⁶⁴

Air Force, Naval, and Marine Corps IG officials stated that they are currently in the process of updating their guidance to better incorporate confidentiality protections. For example, Naval IG officials told us that the Naval IG is updating its Hotline instruction, which will provide guidance to obtain consent from complainants prior to releasing investigation reports to installation commanders or other military officials, or redact the complainant's name. According to Naval IG officials, the updated instruction should be finalized in the first quarter of fiscal year 2019.

CIGIE Quality Standards for Federal Offices of Inspector General state that IGs should establish and follow policies and procedures for receiving and reviewing allegations and ensure that whistleblower identities are not disclosed without consent, unless the IG determines that such disclosure is unavoidable during the course of the investigation. Further, *CIGIE Quality Standards for Investigations* state that policies and procedures

⁶³ Specifically, Air Force Instruction 90-301, *Inspector General Complaints Resolution*, was updated in August 2015; Marine Corps IG Investigations Guide and Concepts and Systems Guide were both updated in August 2009; and the Secretary of the Navy Instruction 5370.5B, *DON Hotline Program*, which provides guidance to both Naval IG and Marine Corps IG Hotlines, was updated in November 2004.

⁶⁴ SECNAVINST 5370.5B.

should be revised regularly to align with current laws and regulations, and that confidentiality should be considered throughout an investigation, to include drafting reports, validating contents, and submitting the final report. Without updated policies and procedures that fully implement confidentiality standards for complaint handling and investigation, the Air Force IG, the Naval IG, and the Marine Corps IG may not be able to ensure the consistent implementation of confidentiality protections within their offices.

IGs Are Able to Access Whistleblower Information to Perform Their Duties and Have Taken Some, but Not All, Required Steps to Safeguard It

IGs Are Able to Access Information Needed to Handle Whistleblower Complaints, and Have Taken Steps to Safeguard Classified Information

DODIG and military service IGs do not experience significant challenges in accessing sensitive or classified information necessary to handle whistleblower complaints, according to cognizant IG officials. Such information includes documentary evidence or witness statements. Similarly, 79 of 86 (92 percent) DODIG respondents to our survey reported that they are generally able to access all types of unclassified information necessary to perform the duties of their position, while 82 of 86 (95 percent) respondents stated that they are either able to access classified information as necessary or do not require access to classified information.

DODIG and the military service IGs have also taken steps to safeguard physical and electronic classified whistleblower information in accordance with DOD policy, which requires that DOD components establish a system of technical, physical, and personnel controls to ensure access to classified information is limited to authorized persons.⁶⁵ Cases including

⁶⁵ DOD Manual 5200.01 Vol.3, *DOD Information Security Program: Protection of Classified Information* (Feb. 24, 2012) (Incorporating change 2, Mar. 19, 2013).

classified information constituted a small percentage of cases closed by DODIG and the military service IGs in fiscal year 2017, with the percentage of those closed by DODIG directorates—including the DOD Hotline and the whistleblower reprisal and senior official investigations—ranging from 0.2 percent to 0.5 percent, according to DODIG officials.⁶⁶ Officials from each of the military service IGs reported closing no classified cases in fiscal year 2017. In addition, DODIG and military service IG officials reported having an adequate number of staff with clearances at the requisite levels (e.g., SECRET) to handle classified case information, along with processes for physically and electronically storing and accessing information at different classification levels.

Most IGs are Following DOD's IT Risk Management Process

DODIG and most military service IGs are following DOD's IT risk management process, which involves the assessment of and authorization to operate IT used to manage DOD information—including sensitive but unclassified whistleblower information.⁶⁷ The Naval IG has not authorized its case management system in accordance with DOD policy, which implements NIST⁶⁸ and Office of Management and Budget⁶⁹ federal IT security guidelines related to IT systems and applications, including those used by the IGs.⁷⁰ However, it is taking steps to do so. DODIG and the Naval IG use IT systems to manage sensitive whistleblower information, while the Air Force, Army, and Marine Corps

⁶⁶ Cases closed by DODIG could include reprisal or misconduct cases involving military service or defense intelligence component personnel for which DODIG has chosen to exercise its discretionary authority to investigate.

⁶⁷ See DOD Instruction 8510.01.

⁶⁸ See National Institute of Standards and Technology, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans*, Special Publication 800-53A, Revision 4 (December 2014); *Security and Privacy Controls for Federal Information Systems and Organizations*, Special Publication 800-53, Revision 4 (April 2013); and *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, Special Publication 800-37, Revision 1 (February 2010).

⁶⁹ Office of Management and Budget, Circular No. A-130, *Managing Federal Information as a Strategic Resource*, (July, 2016).

⁷⁰ An information system is a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. An application is a software program hosted by an information system. See Committee on National Security Systems Instruction No. 4009, *Committee on National Security Systems (CNSS) Glossary* (Apr. 6, 2015).

DODIG and Naval IG IT Systems

IGs use IT applications—which are not subject to the full IT risk management authorization process, as discussed below.

DODIG has followed the DOD IT risk management process by authorizing the Defense Case Activity Tracking System (D-CATS)—its whistleblower case management system—to operate in accordance with DOD policy and federal IT security guidelines. DOD’s risk management process requires that IT systems be authorized to operate using a multistep process that entails the identification, implementation, and assessment of system security controls, along with the corresponding development and approval of a system security plan, security assessment report, and plan of action and milestones.⁷¹ The process requires systems to be reassessed and reauthorized every 3 years in order to ensure the continued effectiveness of security controls, and allows for ongoing authorizations through a system-level strategy for the continuous monitoring of security controls employed within or inherited by the system. The strategy should include a plan for annually assessing a subset of system security controls. DOD policy states that component heads may only operate systems with a current authorization to operate, and that authorization termination dates must be enforced.

DODIG last authorized D-CATS to operate in May 2017, determining that overall system security risk was acceptable based on a review of the system security plan, security assessment report, and plan of action and milestones. Our review of DODIG’s system authorization documents also found that they addressed key, required content elements. For example, the system security plan specified the security controls intended to be in place based on the system’s risk classification, and the security assessment report documented findings of compliance and the methods used by the assessor to evaluate security controls when implementing

⁷¹ An authorization to operate is issued when a system’s authorizing official reviews the system authorization package and deems the risks associated with the system acceptable. The security authorization package documents the results of the security control assessment and provides the authorizing official with information needed to make a risk-based decision on whether to authorize operation of an information system. The authorization package includes a (1) security plan that provides an overview of security requirements, a description of agreed-upon security controls, and other supporting security-related documents; (2) security assessment report that provides the security control assessment results and recommended corrective actions for control weaknesses; and (3) plan of action and milestones that describes the measures planned to correct weaknesses or deficiencies and to reduce or eliminate known vulnerabilities.

DODIG's continuous monitoring strategy.⁷² Additionally, the plan of action and milestones identified tasks needed to mitigate identified vulnerabilities along with resources and milestones to accomplish the tasks.

However, as of December 2018, the Naval IG had not authorized its case management system in accordance with the DOD risk management process, and the system remained in operation.⁷³ The Naval IG was issued an interim authorization to operate its case management system in March 2017 by the Commander, U.S. Fleet Cyber Command. The interim authorization—which expired in January 2018—required the Naval IG to transition from the department's prior IT risk management process to the current process by the time of its expiration, noting that the overall risk of the system was high due to incomplete testing.⁷⁴ Subsequently, in June 2018, the Naval IG requested and was eventually granted, in September 2018, a conditional authorization to continue operating the case management system through October 2018.

In early December 2018, the Naval IG requested another conditional authorization to operate the case management system until September 2019. According to Naval IG officials, the conditional authorization is needed because the whistleblower case management system's host environment is not expected to attain its authorization until September 2019. As a result, the Naval IG was taking steps beyond the conditional authorization request to manage IT security risks as it works towards compliance with the new DOD risk management process. For example, Naval IG officials stated that new leadership was put in place to oversee the case management system; that a senior system administrator would be hired to help maintain IT security; and that the case management

⁷² DODIG included these procedures in a separate document. We did not assess the sufficiency of the evaluation methods.

⁷³ The Naval IG is the only military service IG that operates a case management system instead of an application under the DOD IT risk management process categorization rules.

⁷⁴ DOD Instruction 8510.01 requires that DOD components transition to the current DOD risk management process within two-and-a-half years from the component's last authorization under the prior DOD Information Assurance Certification and Accreditation Process, which could be used until October 2016.

system was undergoing regular scans to assess security risks, with any resultant issues being remediated.⁷⁵

NIST guidelines state that organizations should design and prioritize activities to mitigate security risks, and that alternative strategies may be needed when an organization cannot apply controls to adequately reduce or mitigate risk.⁷⁶ As noted, the Naval IG's case management system was not authorized as of December 2018 and it was not yet able to transition to the current DOD risk management process. However, if completed, the actions planned and underway—including the conditional authorization and security scans—should help to mitigate system security risks and provide greater assurance that existing system security controls safeguard sensitive whistleblower information.

Air Force, Army, and Marine Corps IG IT Applications

The IGs of the Air Force, the Army, and the Marine Corps are following DOD's IT risk management procedures for their primary case management applications, which are not subject to the full IT risk management authorization process. According to DOD Instruction 8510.01, *Risk Management Framework (RMF) for DOD Information Technology (IT)*, DOD IT such as applications must be securely configured in accordance with applicable DOD policies, and application security controls must undergo special assessment of their functional and security-related capabilities and deficiencies. The results of such assessments are to be documented within an application-level security assessment report and reviewed by a security manager to ensure that the product does not introduce vulnerabilities into its host system.

We found that while the Army, Air Force, and Marine Corps IGs have not produced the required application-level security assessment reports for their primary applications, they have met the intent of these requirements through other actions. Specifically, we noted that the Air Force and Army IGs' primary case management applications reside in host systems that were authorized to operate under the risk management process within the last 3 years, and that the assessments associated with the host system

⁷⁵ Naval IG officials stated that the ongoing efforts to reauthorize the case management system would not have been required if the enterprise case management system being developed by DODIG had been released according to its original schedule. As discussed later in this report, the enterprise system will replace the IT systems and applications currently used by the military service IGs, but its incremental release schedule has been delayed.

⁷⁶ National Institute of Standards and Technology, Special Publication 800-53, Revision 4.

authorizations included a review of application-level security controls, according to IG officials.⁷⁷ Similarly, the Marine Corps IG's case management application was exempted from assessment by its authorizing official because it was determined that the application did not introduce additional risk into its authorized host system.

DODIG Does Not Fully Restrict Employee Access to Sensitive Whistleblower Information

DODIG's Case Management System Does Not Include Some Controls to Restrict Internal Employee Access

As previously discussed, DODIG has taken steps to restrict employee access to whistleblower information, such as by restricting access to cases in which a complainant has not consented to releasing his or her identity. DOD Hotline also applies additional restrictions to all cases involving internal misconduct referrals to the Office of Professional Responsibility and CIGIE Integrity Committee, and it has the capability to further restrict records, according to DODIG officials. Beyond restricting records, the case management system also includes user roles, which govern users' view of information. However, employees at the three DODIG directorates that are principally responsible for handling whistleblower information are generally able to access sensitive whistleblower information belonging to other directorates in both the Defense Case Activity Tracking System (D-CATS)—DODIG's whistleblower case management system—and an associated document repository, that is not necessary to accomplish assigned tasks. NIST Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, states that organizations should employ the core security principle of *least privilege*, which allows only authorized access for users that is necessary to accomplish assigned

⁷⁷ The Air Force's case management application resides in a system that was granted a conditional authorization to operate in March 2018. The conditional authorization was contingent on the implementation of all system baseline security controls, monthly updates to the plan of action and milestones, and the submission of an approved continuous monitoring strategy. As of August 2018, these conditions had generally not been met, according to Air Force officials. However, these same officials stated that the Air Force IG was working with the authorizing official to address shortfalls and that a denial to operate had not been issued. Additionally, these officials noted that the application's host system would also be moving to a new environment by December 2018, at which point a new assessment would be needed.

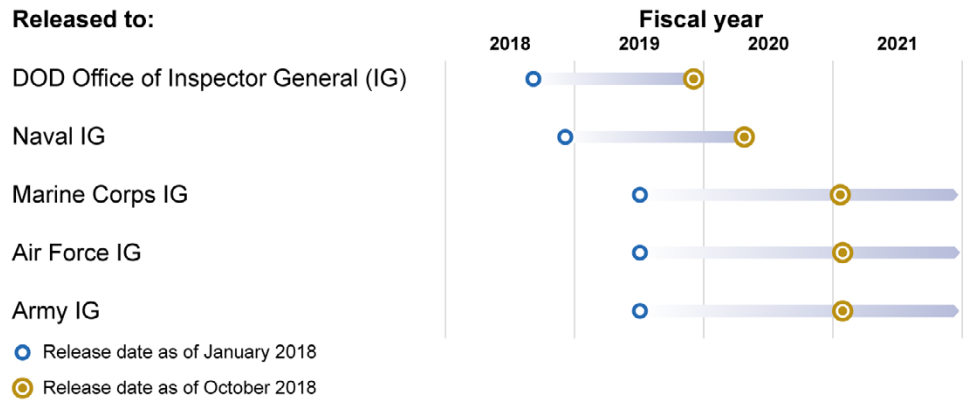
tasks in accordance with organizational missions and business functions.⁷⁸

DODIG employees in the DOD Hotline, senior official investigations directorate, and whistleblower reprisal investigations directorate are able to access whistleblower information belonging to other DODIG directorates in both D-CATS and its associated document management repository because DODIG has not developed sufficient system controls needed to restrict access across the three directorates. For example, a DODIG employee in either the senior officials or reprisal investigations directorates can access Hotline records in D-CATS that the employee does not have a need to access, with the exception of cases specifically restricted by the DOD Hotline to prevent unauthorized access. According to an August 2018 internal DODIG memo, the lack of controls to restrict access to information across the three directorates has been known since the system was established in 2012.

DODIG plans to establish controls to restrict access among the DODIG directorates in a new enterprise system (D-CATSe), which will eventually replace D-CATS and the case management systems used by the military service IGs. D-CATSe is intended to provide a common case activity tracking system capable of supporting mandatory reporting requirements and collecting, storing, and exchanging IG records related to complaints and administrative investigations throughout a complaint's lifecycle. According to DODIG officials, D-CATSe will restrict access both within and among user IGs, including the DODIG directorates and military service IGs, each of which may have unique access requirements based on their different types of user groups. According to DODIG officials, this will be accomplished through the establishment of unique business units at different organizational levels, teams, and user roles, which will collectively determine what information a user can access. However, as shown in figure 7 below, the incremental release schedule for D-CATSe has been delayed, and the IGs are not expected to fully transition to the new system until fiscal year 2021.

⁷⁸ National Institute of Standards and Technology, Special Publication 800-53, Revision 4.

Figure 7: Change in Defense Case Activity Tracking System enterprise Projected Release Dates Between January and October 2018



Source: GAO analysis of Department of Defense Office of Inspector General (DODIG) information. | GAO-19-198

NIST guidelines state that organizations should design and prioritize activities to mitigate security risks, and that alternative strategies (such as plans) may be needed when an organization cannot apply controls to adequately reduce or mitigate risk.⁷⁹ Further, NIST guidelines state that addressing assurance-related controls⁸⁰ during system development can help organizations obtain sufficiently trustworthy information systems and components that are more reliable and less likely to fail.⁸¹ However, DODIG does not plan to take other actions to address the lack of cross-directorate controls before the advent of the enterprise system. Additionally, while DODIG is designing such controls and plans for each system release to provide a requirements basis for subsequent releases, it has not developed an assurance plan for testing controls, according to DODIG officials, or fully defined the system requirements needed to implement these controls and ensure it has achieved least privilege both within and across the user IGs. Without considering interim actions to address the lack of D-CATS cross-directorate access controls, DODIG may be unable to sufficiently mitigate security risks while D-CATSe is developed. Also, without developing a plan with assurance controls for achieving least privilege in D-CATSe, DODIG may be unable to ensure

⁷⁹ National Institute of Standards and Technology, Special Publication 800-53, Revision 4.

⁸⁰ Assurance is the grounds for justified confidence that a security or privacy claim has been or will be achieved. See National Institute of Standards and Technology, Special Publication 800-37, Revision 2.

⁸¹ National Institute of Standards and Technology, Special Publication 800-53, Revision 4.

the confidentiality and integrity of sensitive whistleblower information during its implementation.

DODIG Has Identified Instances Involving Improper Employee IT Access Rights to Whistleblower Information

Separate from the lack of cross-directorate controls, DODIG has identified multiple instances in which sensitive but unclassified whistleblower information in the DODIG Administrative Investigations directorate whistleblower case management system and document repository was accessible to DODIG personnel who did not have a need to know this information. These instances involve DOD Hotline records that are specifically restricted to protect complainants requesting confidentiality, along with records belonging to DODIG’s Office of Professional Responsibility—which handles internal DODIG misconduct complaints.

Table 6 shows examples of recent instances in which DODIG determined that sensitive whistleblower records were accessible to DODIG personnel without a need to know. According to DODIG officials, as of January 2019, there were no known instances of anyone without a need to know actually accessing these records.⁸² These officials also stated that corrective action had been taken for each instance in table 6, including by blocking access to information while the underlying issues were resolved; that at no time was information available to the public; and that the instances did not result in any disclosure outside of DODIG.

Table 6: Select Accessibility Issues Identified by DODIG from November 2017 through May 2018

Instance
Numerous restricted records in DODIG’s whistleblower document repository were accessible to DODIG administrative investigations personnel without a need to know, including through an intranet search.
946 folders in DODIG’s document repository were accessible to DODIG employees formerly with DOD Hotline and the senior officials and whistleblower reprisal investigations directorates. ^a
Restricted DOD Hotline records were accessible to unauthorized DODIG employees in the DODIG’s document repository.
Two case records belonging to DODIG’s Office of Professional Responsibility were accessible to DOD Hotline staff in the case management system. ^b

Source: GAO analysis of Department of Defense Inspector General (DODIG) after-action report and information memorandum to the DODIG Chief of Staff. | GAO-19-198

^aDODIG officials stated that any DODIG employees formerly with the DOD Hotline or senior officials or whistleblower reprisal investigations directorates would likely not have known how to actually access these files because such files are typically accessed through links in D-CATS and because the files would not have been part of the employees’ default view in the document repository.

^bDODIG officials stated that the case records were briefly visible to DODIG employees responsible for handling Hotline complaints, and that DODIG immediately began remediation steps.

⁸² However, DODIG did not provide documentation that improper access was thoroughly investigated in all instances.

NIST guidelines state that the need for certain user privileges may change over time, necessitating the periodic review of assigned user privileges in order to determine if the rationale for assigning such privileges remains valid.⁸³ DODIG has determined that its user access issues are broadly attributable to system administration and application problems, including permission changes resulting from system updates. To address such issues, DODIG has taken several remedial actions and identified additional recommended steps, including:

- reconciling user accounts and validating permissions related to restricted records;
- reviewing policies related to protecting complainant confidentiality and conducting awareness training with personnel, as appropriate; and
- developing enhanced user management procedures and internal controls related to establishing user accounts, reconciling current user permissions, and controlling access to restricted records.

In addition, in October 2018, DODIG instituted a process whereby user privileges associated with its case management system and document repository will be reviewed, validated, and corrected, if necessary, on a quarterly basis. If fully implemented, this process, along with the proposed actions, should help ensure that assigned user privileges are periodically validated and aligned with business needs. However, DODIG's process does not include steps to test document repository permissions after case management system updates, which were determined by DODIG to be the cause of some permission issues.⁸⁴

Without including such steps in its process, DODIG lacks assurance that system permissions will align with business needs on an ongoing basis, and therefore may not be able to appropriately control user accounts to prevent unauthorized access by system users.

⁸³ National Institute of Standards and Technology, Special Publication 800-53, Revision 4.

⁸⁴ A May 2018 internal DODIG after action-report recommended that document repository permissions be thoroughly tested after each case management system update.

Sensitive Whistleblower Information Has Been Accessible to Military Service IG Employees without a Need to Know

The military service IGs’ case management systems and applications incorporate IT controls, such as authenticated user accounts and unique permissions, to protect certain whistleblower information. However, service IG systems and applications do not fully restrict employee access to sensitive whistleblower information only to information that is necessary to accomplish assigned tasks. As previously discussed, NIST guidelines state that organizations should only provide authorized access to users which is necessary to accomplish assigned tasks in accordance with organizational missions and business functions.⁸⁵ As shown in Table 7, DODIG’s quality assurance reviews and our work identified issues related to IG employee access restrictions.

Table 7: Employee Access Issues Involving Military Service IG Information Systems and Applications

Military service IG	Description of access issue
Air Force	DODIG found in its 2017 quality assurance review that the Air Force IG’s application allowed users from other DOD component IGs (such as the Defense Contract Audit Agency IG) to view case descriptions and complainant identities for cases belonging to the Air Force IG, and that it did not restrict the system support contractor from viewing cases that involved its employees.
Army	DODIG found in its 2018 quality assurance review that the Army IG’s application did not restrict Army IG personnel without a need to know from accessing allegations involving Army IG personnel.
Marine Corps	Marine Corps IG officials told us in August 2018 that employees in Marine Corps IG offices were able to see cases assigned to other Marine Corps IG offices without a need to know, and that the application contained other similar malfunctions, such as returning search results for a user other than the user performing the search, within the same IG office.
Naval	DODIG found in its 2016 quality assurance review that the Naval IG’s system did not prevent Naval IG personnel from viewing investigations involving other internal Naval IG personnel, and that it did not adequately restrict employee access to senior official investigations.

Source: GAO analysis of Department of Defense Office of Inspector General (DODIG) and military service IG information. | GAO-19-198

At the time of our review, the military service IGs had not taken steps to fully address the identified access issues. Specifically, Air Force officials stated that they did not plan to address the application access issues because they did not have funding to continue developing their existing application prior to transitioning to D-CATSe, although they would explore whether solutions were possible within current fiscal constraints during the next system maintenance evaluation. Similarly, Army IG officials stated that while the Army IG had resources to further develop its existing case management application, they had elected to not use those resources to remedy the identified access issue in light of the future arrival of D-CATSe. In addition, Naval IG officials reported taking action to

⁸⁵ National Institute of Standards and Technology, Special Publication 800-53, Revision 4.

restrict senior official investigations, but did not provide information to us on actions taken to address DODIG's recommendation to restrict cases involving internal Naval IG personnel. Finally, Marine Corps IG officials stated that access restrictions would be implemented as part of an application redesign scheduled to be complete by the end of 2018. However, these officials also noted that they have not identified the root of the access problem or developed a plan to ensure that needed access restrictions are implemented and functioning properly, raising questions as to whether the redesign will fully restrict access on a continuing basis. As mentioned previously, the Marine Corps' case management application is also exempt from testing under the DOD IT risk management process, and therefore is not subject to routine security assurance testing.

Federal Standards for Internal Control state that management should analyze and respond to risks, and evaluate and remediate internal control deficiencies on a timely basis, including those related to audit findings.⁸⁶ Further, NIST guidelines state that organizations should design and prioritize activities to mitigate security risks, and that alternative strategies, such as plans, may be needed when an organization cannot apply controls to adequately reduce or mitigate risk. These guidelines also encourage organizations to obtain assurance-related evidence on an ongoing basis in order to maintain the trustworthiness of information systems.⁸⁷ As previously discussed, D-CATSe is being implemented incrementally, with releases for the Naval IG and the Air Force and Army IGs not scheduled to occur until fiscal years 2020 and 2021, respectively. By considering actions prior to the advent of D-CATSe, the Air Force, Army, and Naval IGs could mitigate existing risks to whistleblower confidentiality by reducing the potential for unauthorized employee access of whistleblower records. Also, by developing a plan to ensure that access restrictions function properly, the Marine Corps IG could better ensure the confidentiality and integrity of sensitive whistleblower information in its redesigned case management application on a continuing basis.

⁸⁶ [GAO-14-704G](#).

⁸⁷ National Institute of Standards and Technology, Special Publication 800-53, Revision 4.

IGs Report Few Instances of Confidentiality Violations but IT Access Issues Create This Potential

Potential violations of whistleblower confidentiality may be reported to DODIG, the service IGs, the Office of Special Counsel, or CIGIE. IGs identified some substantiated violations of whistleblower confidentiality between fiscal years 2013 and 2018. Specifically, DODIG identified 8 substantiated violations of whistleblower confidentiality between fiscal years 2013 and 2018, representing approximately .01 percent of the 95,613 contacts handled by DODIG during that timeframe, according to DODIG officials.⁸⁸ Army IG identified 6 substantiated violations of whistleblower confidentiality between these years. These violations include the improper release of IG information, disclosures made to individuals who do not have a need to know, and unauthorized access to whistleblower records by IG personnel. DODIG officials noted that in some instances, violations were determined not to result from employee misconduct because the complainant's identity was disclosed unwittingly. According to DODIG and Army IG officials, disciplinary or corrective action was taken in all but one of the 14 substantiated violations because the DODIG employee involved resigned prior to action being taken. Officials from the Air Force, Naval, and Marine Corps IGs stated that they were unaware of any substantiated incidences of confidentiality violations between fiscal years 2013 and 2018 and that they were unable to specifically track such incidents in their case management systems.⁸⁹ Similarly, CIGIE Integrity Committee and Office of Special Counsel officials stated that they were unaware of and do not specifically track confidentiality violations, and we did not identify any confidentiality violations in the fiscal year 2013-2018 data they provided to us that involved DODIG employees.⁹⁰

⁸⁸ DODIG officials stated that they manually reviewed case data in order to identify potential violations, but that a future release of DODIG's case management system will include an automated capability to track allegations of compromising IG source identities with a specific field checkbox.

⁸⁹ A senior Marine Corps official recalled one potential violation of confidentiality, wherein IG staff provided a protected communication to the alleged subject. According to this official, the potential violation was not fully investigated because the IG staff that allegedly shared the information was terminated from his or her position.

⁹⁰ To address our mandate, we also asked DODIG about the extent of retaliatory investigations involving DODIG employees between fiscal years 2013 and 2018. DODIG officials stated that there were no known incidences of retaliatory investigations, and we did not identify any such instances in the fiscal years 2013-2018 data we reviewed on cases involving DODIG employees from DOD Hotline, the DODIG Office of Professional Responsibility, the CIGIE Integrity Committee, or the Office of Special Counsel.

Respondents to our survey of DODIG employees separately reported potential violations of whistleblower confidentiality.⁹¹ Specifically, 15 of the 86 respondents (about 17 percent) reported being aware of at least one instance since June 1, 2017, where the identity of a complainant or source was avoidably disclosed by a DODIG employee to an organization or individual without a need to know, and nine of these 15 were aware of more than one instance. These responses are not intended to be a count of separate instances because respondents may have recalled the same instance(s), including one or more of the 8 substantiated violations reported to us by DODIG. The most common avoidable disclosure described by survey respondents involved distributing whistleblower materials to the wrong official or agency. Survey respondents reported that in such instances corrective action included recalling the complaint and deleting the erroneously sent record, or, in some cases, sending a complaint to DODIG's Office of Professional Responsibility for the investigation of possible misconduct.

While the number of known violations is small, IT access issues related to the case management systems and applications used by DODIG and the military service IGs create the potential for additional violations of whistleblower confidentiality.⁹² As previously discussed, issues such as the absence of cross-directorate access controls within DODIG's case management system and the ability for non-Air Force IG users of the Air Force IG case management system to view IG case information allow for the improper access of sensitive whistleblower information. Recognizing this potential, a senior DODIG official noted concern regarding the possible extent of confidentiality violations stemming from these and the other access issues previously discussed in this report. Additionally, DODIG requested that the Defense Criminal Investigative Service investigate the April 2018 incident involving 946 case folders to determine who accessed the identified records. Without steps to address these

⁹¹ As noted, these are potential violations of whistleblower confidentiality. We did not independently assess the specifics of the avoidable disclosures reported by survey respondents.

⁹² DOD's privacy program defines lost, stolen or compromised information or a breach of information as an actual or possible loss of control, unauthorized disclosure, or unauthorized access of personal information where persons other than authorized users gain access or potential access to such information for an other than authorized purpose where one or more individuals will be adversely affected. See DOD 5400.11-R *Department of Defense Privacy Program* (May 14, 2007).

ongoing IT access issues, the potential for additional violations of whistleblower confidentiality will persist.

DODIG Generally Met Documentation Requirements in Senior Official Cases that GAO Reviewed and Reported Most Credible Allegations

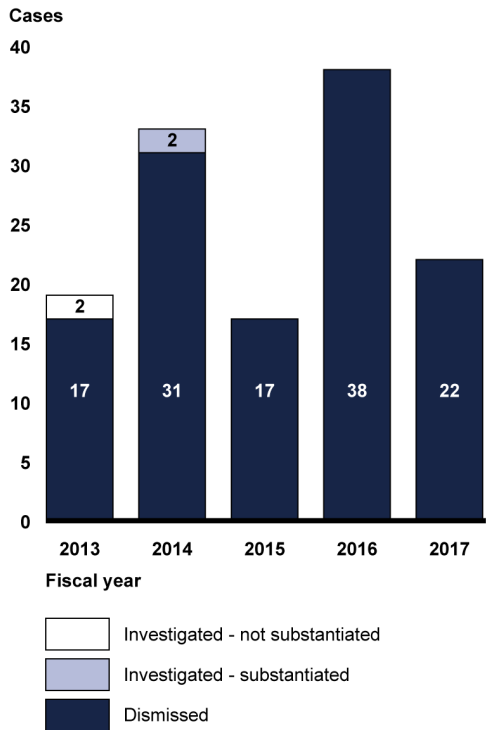
DODIG Dismissed Most Cases Involving Civilian DOD Presidential Appointees with Senate Confirmation and Generally Included Required Data and Documentation

DODIG closed 129 misconduct and reprisal cases in fiscal years 2013 through 2017 with complaints involving a civilian DOD Presidential appointee with Senate confirmation (PAS)⁹³ subject.⁹⁴ Of the 129 cases closed, DODIG dismissed without investigation 125 cases and investigated the remaining four. Figure 8 shows the number of cases closed in each fiscal year, by case disposition.

⁹³ PAS positions include cabinet secretaries, agency heads, and undersecretary-level posts.

⁹⁴ Appendix III presents data on the characteristics of the 129 closed cases, including closure dates, allegation types, and organizational source.

Figure 8: Disposition of DODIG Closed Misconduct and Reprisal Cases Involving Civilian DOD Presidential Appointees with Senate Confirmation, Fiscal Years 2013–2017



Source: GAO analysis of the Department of Defense Office of Inspector General (DODIG) data. | GAO-19-198

Our review of the 125 case files for dismissed misconduct and reprisal cases found that key documentation and data needed to demonstrate compliance with significant aspects of the case-handling process were generally present. Key documentation and data for dismissed cases include the case open and close dates, the incoming complaint, disposition of the case, and the dismissal approval and rationale.⁹⁵ CIGIE standards state that the degree to which an organization efficiently achieves its goals is affected by the quality and relevance of information that is collected, stored, retrieved, and analyzed, and that the results of investigative activities should be accurately and completely documented in the case file.⁹⁶

⁹⁵ See appendix I for a more detailed description of our casefile review methodology.

⁹⁶ CIGIE, *Quality Standards for Investigations* (Nov.15, 2011).

Examples of data and documentation consistently present. Our review of 125 case files for dismissed cases closed in fiscal years 2013 through 2017 found that key documentation and data were generally present. For example:

- 100 percent of the cases we reviewed included the incoming complaint.
- Approximately 99 percent of the dismissed misconduct cases included a dismissal rationale that aligned with dismissal criteria in DODIG policy.⁹⁷
- 100 percent of the dismissed reprisal cases that involved a closure letter informing the complainant of case dismissal listed a rationale for dismissal in the closure letter.
- 100 percent of the dismissed reprisal cases that did not involve a closure letter to the complainant had a rationale for dismissal elsewhere in the case file.
- Approximately 99 percent of dismissed misconduct cases included a required entry recording the intake disposition.⁹⁸

Documents or data that were not material. Our review of case files for dismissed cases closed in fiscal years 2013 through 2017 found that some other documentation or data that are needed to demonstrate compliance with DODIG policy were missing. The deficiencies we found were not material to case outcomes. For example, approximately 77 percent of dismissed misconduct cases did not include a recording of case dismissal approval by IG supervisory staff. However, DODIG officials told us that the presence of the required entry recording the intake disposition indicated that the case dismissal had been approved by the appropriate authority. Similarly, approximately 55 percent of dismissed misconduct cases did not include a notification letter to the appropriate military service IG in the case file. DODIG officials stated that

⁹⁷ DODIG dismissal criteria for not investigating cases involving senior official subjects include a determination of whether the allegations are credible and whether the allegations, if proven true violate criminal law. See Office of the Deputy Inspector General for Administrative Investigations, *AI Investigations Manual* (2012) and *AI Investigations Manual* (Mar. 29, 2016).

⁹⁸ Intake disposition includes the decisions to accept, decline, or refer a case as well as approval and rationale for dismissals, among other things.

while there is guidance to send these letters, it is not a required practice.⁹⁹

DODIG Has Reported Most Credible Misconduct Allegations to the Secretary of Defense and Some Investigation Results to Congress

DODIG reported most credible allegations concerning civilian DOD PAS officials to the Secretary of Defense as required. DODIG also reported some investigation results involving these officials to Congress prior to the enactment of the Inspector General Empowerment Act of 2016, which required the reporting of results of substantiated investigations involving DOD senior officials.¹⁰⁰ DODIG investigated four of the 129 cases closed in fiscal years 2013 through 2017, with two of those investigations leading to substantiated allegations of misconduct.

DODIG generally met DOD requirements to report credible allegations of misconduct against civilian DOD PAS officials to the Secretary of Defense. DOD Directive 5505.06 requires that DODIG notify the Secretary of Defense of all credible allegations or investigations involving presidential appointees and others of significance, including Senate-confirmed civilian officials.¹⁰¹ We found documentary evidence that DODIG notified the Secretary of credible allegations in three of the four misconduct and reprisal investigations closed from fiscal years 2013 through 2017, and the secretary of a military service was notified in the fourth case. In addition, DODIG officials stated that the Principal Deputy IG provides the Secretary of Defense periodic updates on current investigations and other periodic updates of incoming allegations, as necessary and appropriate.

Separately, the Inspector General Empowerment Act of 2016 requires that DODIG report in its semiannual reports to Congress on all substantiated allegations of misconduct involving senior officials. Prior to 2016, there was no requirement to notify Congress of substantiated

⁹⁹ DODIG, *Investigations of Senior Officials Defense Case Activity Tracking System User Guide* (October 2015).

¹⁰⁰ The Inspector General Empowerment Act of 2016, Pub. L. No. 114-317 (2016) amended the Inspector General Act of 1978, at 5 U.S.C. Appendix by requiring that IG semi-annual reports to Congress include a report on each investigation conducted by the office involving a senior government employee where allegations of misconduct were substantiated, and including in the report a detailed description of the facts and circumstances of the investigation and the status and disposition of the matter, including whether the matter was referred to the Department of Justice.

¹⁰¹ DOD Directive 5505.06.

allegations of misconduct involving senior officials. We found evidence that DODIG communicated investigation results to Congress in two of the four civilian DOD PAS official investigations closed between fiscal years 2013 and 2017, but not in the other two because it was not required.¹⁰² For one investigated case, a report of investigation was provided to Congress upon request, and for another investigation, which had a substantiated allegation, the results of the investigation were published in narrative detail in a semi-annual report to Congress. DODIG now reports in its semi-annual reports to Congress summary results of substantiated and unsubstantiated cases closed during the corresponding period, but it has not closed any civilian DOD PAS official allegations since the statutory requirement to report to Congress on all substantiated cases was established.

Conclusions

Maintaining a program that instills trust and confidence for potential whistleblowers to come forward is critical to minimizing fraud, waste, abuse, and personnel misconduct in the federal government. Important components of a credible whistleblower program are timeliness of case processing and safeguarding confidentiality to the maximum extent possible. It is encouraging that DODIG and the service IGs have met some key goals and have policies that address whistleblower confidentiality. In addition, DODIG generally met key documentation and data requirements for the 125 cases dismissed by DODIG involving civilian DOD PAS officials, and reported most credible allegations, as required.

However, the IGs face challenges in addressing unmet timeliness goals and updating guidance to ensure full alignment with current confidentiality requirements. By pursuing more targeted, collective efforts with additional initiatives aimed at improving performance against unmet timeliness goals, the IGs can better assure current and potential whistleblowers that their complaints will be processed expeditiously. Additionally, without formal guidance documenting procedures for protecting the confidentiality of whistleblowers reporting potential internal DODIG employee misconduct, those employees lack assurance that DODIG can fully protect their identities. Similarly, without updated policies and procedures,

¹⁰² DODIG officials stated that all four cases were included in summary statistics reported to Congress in semiannual reports, and that DODIG's Office of Legislative Affairs and Communication may have received and responded to Congressional requests related to one or more of the four cases.

the Air Force, Naval, and Marine Corps IGs may not be able to fully ensure whistleblower confidentiality in their organizations.

The integrity of a whistleblower program also extends to ensuring that sensitive information in IT systems remains secure and inaccessible by employees without a need to know. The IGs have existing controls for safeguarding whistleblower information, but additional efforts are warranted. Specifically, without further steps—such as considering interim actions to mitigate the lack of cross-directorate access controls, developing a plan, along with the military service IGs for achieving least privilege in the future enterprise case management system, and enhancing the process for periodically validating user privileges—DODIG may not be able to ensure that access controls in its existing and future case management systems align with business needs on an ongoing basis. Similarly, without considering actions to further restrict IG employee access in existing IT, the Air Force, Army, and Naval IGs may be unable to mitigate ongoing risks to whistleblower confidentiality. Finally, without a plan for ensuring that access restrictions in its redesigned case management system function properly, the Marine Corps IG may be unable to fully ensure whistleblower confidentiality.

Recommendations for Executive Action

We are making a total of 12 recommendations to DOD. Specifically:

The DOD Inspector General should coordinate with the IGs of the military services to take additional actions to improve performance against unmet timeliness goals. This includes steps to improve performance of senior official misconduct investigations and military service reprisal intakes, and to resolve disagreement on notifications. (Recommendation 1)

The DOD Inspector General should issue formal guidance documenting procedures for protecting the confidentiality of whistleblowers throughout its internal misconduct investigation process. (Recommendation 2)

The Air Force Inspector General should establish procedures to fully reflect and implement DOD policy on the protection of whistleblower confidentiality. (Recommendation 3)

The Marine Corps Inspector General should establish procedures to fully reflect and implement DOD policy on the protection of whistleblower confidentiality. (Recommendation 4)

The Naval Inspector General should establish procedures to fully reflect and implement DOD policy on the protection of whistleblower confidentiality. (Recommendation 5)

The DOD Inspector General should consider interim actions as the whistleblower enterprise case management system is being developed to help ensure that access to sensitive whistleblower information in the current case management system and associated document repository is limited to information that is necessary to accomplish assigned tasks. (Recommendation 6)

The DOD Inspector General should coordinate with the IGs of the military services to develop a plan to fully restrict case access in the future whistleblower enterprise case management system so that user access is limited to information necessary to accomplish assigned tasks in accordance with organizational missions and business functions. (Recommendation 7)

The DOD Inspector General should enhance its process for periodically reviewing whistleblower case management system and document repository user privileges by including steps to ensure that such privileges remain valid after system updates, as appropriate. (Recommendation 8)

The Air Force Inspector General should consider interim actions as the whistleblower enterprise case management system is being developed to help ensure that access for users of existing applications is limited to information that is necessary to accomplish assigned tasks in accordance with organizational missions and business functions. (Recommendation 9)

The Army Inspector General should consider interim actions as the whistleblower enterprise case management system is being developed to help ensure that access for users of existing applications is limited to information that is necessary to accomplish assigned tasks in accordance with organizational missions and business functions. (Recommendation 10)

The Marine Corps Inspector General should develop a plan to ensure that its redesigned whistleblower case management application restricts user access to information based on what is needed to accomplish assigned tasks in accordance with organizational missions and business functions. (Recommendation 11)

The Naval Inspector General should consider interim actions as the whistleblower enterprise case management system is being developed to help ensure that access for users of existing applications is limited to information that is necessary to accomplish assigned

tasks in accordance with organizational missions and business functions. (Recommendation 12)

Agency Comments and Our Evaluation

We provided a draft of this report to DODIG and the military service IGs for review and comment. In written comments, DODIG and the military service IGs concurred with each of our 12 recommendations. Comments from DODIG and the Air Force, Army, and Marine Corps IGs are reproduced in appendix V; the Naval IG concurred in an email. These IGs also provided technical comments, which we have incorporated as appropriate.

In its comments, DODIG stated that it will seek to implement the recommendations. In addition to highlighting recent and planned improvements, DODIG provided additional comments on some of the report's findings and statements. In particular, DODIG noted that the report understated its improvements in timeliness, such as by stating that DODIG did not meet timeliness goals related to average days of senior official and military reprisal intakes, and average days for reprisal oversight reviews. Citing figure 2, DODIG further stated that it met its timeliness goals in more than 60 percent of all senior official and reprisal intake cases, including 87 percent of senior official oversight review cases, and that it met its 15-day goal in more than 70 percent of senior official intakes. We agree that DODIG achieved these percentages and present the associated data in figure 2. However, as described in the report, and shown in figure 2, DODIG did not meet its goals for the average days of senior official misconduct and military reprisal intakes, and the average days for reprisal oversight reviews. Nonetheless, it is encouraging that DODIG has taken and planned actions to improve timeliness as its caseload has increased, including by increasing its staff by about 29 percent since fiscal year 2016, during which time it reported that its caseload similarly increased by about 26 percent.

DODIG also noted that the report presented some information in a manner that could create an incomplete impression of the agency's commitment to protecting whistleblower confidentiality. Specifically, DODIG stated that the report's presentation of survey data related to DODIG employee concerns about internal DODIG processes may give a misleading impression because of the focus on the small number of respondents who had a negative impression. In particular, DODIG noted that more than 80 percent of respondents either believed that DODIG's internal process for reporting misconduct protected confidentiality somewhat or very well, or did not know if it did so. However, a positive

perspective cannot be inferred from the respondents that reported not knowing whether or not DODIG's internal process protects confidentiality (42 percent). Also, it should be recognized that the respondents that held negative views on DODIG's process for reporting internal misconduct (16 percent) accounted for a substantial proportion of respondents (28 percent) that held either positive or negative views on this issue. Importantly, these and other survey information presented in the report also provide valuable information on the degree to which DODIG employees have confidence in the integrity of these important internal processes, and, as mentioned, align with other information obtained during our review. As such, this information may help to inform DODIG's efforts in addressing our recommendation to issue formal guidance documenting procedures for protecting the confidentiality of whistleblowers throughout its internal misconduct process, along with any future efforts to instill employee confidence in internal misconduct reporting mechanisms.

DODIG also noted that portions of the report addressing restrictions on DODIG employee access to sensitive whistleblower records need further context, stating specifically that no DODIG employees outside of the Administrative Investigations directorate, Office of Professional Responsibility, and Office of General Counsel had access to any of the records, and that there was no evidence that any person without a need to know accessed any such records. However, information provided to us by DODIG does not show that accessibility was limited in all instances to employees within one of those DODIG offices. Also, the ability of any employee to access records that were specifically restricted to protect complainant identities or internal records belonging to the Office of Professional Responsibility is problematic given the increased sensitivity of such records. Further, while DODIG did not identify instances in which anyone without a need to know accessed the records, DODIG did not provide evidence that all cases of improper access were thoroughly investigated, as we state in our report, and the instances included in the report are examples and not inclusive of all instances of improper access identified by the DODIG. Nevertheless, it is positive that DODIG has reported taking corrective action to address instances of improper accessibility. It is also encouraging that DODIG plans to implement our recommendations, as the potential for unauthorized access will persist until it establishes cross-directorate controls in the case management system and enhances its processes for periodically reviewing user privileges for its whistleblower case management system and document repository.

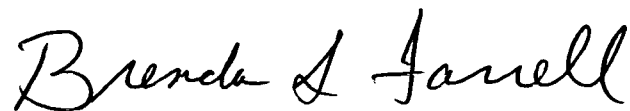
All of the military service IGs concurred with the recommendations directed to them. The Air Force and the Army IGs also provided comments on some of the report findings. In particular, the Air Force IG noted in relation to our third recommendation that language in Air Force Instruction 90-301, updated in December 2018, is essentially the same as 5 U.S.C. Appendix § 7, and that this language precludes Air Force officials at any level from waiving the requirement to inform complainants and employees of the requirement to not disclose their identities without their consent, unless the Inspector General determines such disclosure to be unavoidable. However, as stated in our report, Air Force guidance did not include requirements outlined in DOD Instruction 7050.01 related to the specific conditions under which information disclosures may be made without complainant consent. These include circumstances wherein a complainant has made it known outside IG channels that he or she submitted the complaint, there is an emergency situation or health or safety issue, or the allegation is being transferred outside of DOD to another IG. As a result, we continue to believe that without updated policies and procedures that fully implement confidentiality standards, the Air Force IG may not be able to ensure the consistent implementation of confidentiality protections.

Separately, in relation to IG employee access of information, the Army IG stated that the processes it has in place provide judicious access and control of whistleblower information to achieve an appropriate balance between efficient operations and minimized risk. As stated in our report, DODIG's 2018 quality assurance review of the Army IG found that the Army IG's application did not restrict personnel without a need to know from accessing allegations involving Army IG personnel, contrasting with NIST guidelines, which predicate user access on the need to accomplish assigned tasks. Army IG officials acknowledged this issue, but stated that the Army IG had elected to not use existing resources to further develop its case management application in light of the enterprise system being developed by DODIG. As a result, we continue to believe that by considering actions prior to the advent of the enterprise system—which is not expected to be released to the Army IG until fiscal year 2021—the Army IG could mitigate risks to whistleblower confidentiality by reducing the potential for unauthorized IG employee access of whistleblower records.

We are sending copies of this report to congressional committees; the Acting Secretary of Defense; the Department of Defense Principal Deputy Inspector General performing the duties of the Inspector General; the

Inspectors General of the Air Force, the Army, the Navy, and the Marine Corps; the Office of Special Counsel; and other interested parties. In addition, the report is available at no charge on the GAO website at <http://www.gao.gov>.

If you or your staff have any questions about this report, please contact me at (202) 512-3604 or farrellb@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix VI.



Brenda S. Farrell
Director
Defense Capabilities and Management

Appendix I: Scope and Methodology

To determine the extent to which the Department of Defense Office of Inspector General (DODIG) and the military service offices of inspector general (IG) met and took steps to achieve key fiscal year 2018 timeliness and quality goals related to the handling of whistleblower complaints, we reviewed performance documentation and interviewed officials on DODIG and military service IG timeliness and quality goals, performance measures, and associated performance data for fiscal year 2018, along with ongoing and planned efforts to improve performance. We also reviewed fiscal year 2017 performance data for comparison purposes. We selected data from this period because they constituted the most complete and recent performance data available. Using the data, we assessed the extent to which DODIG and the military service IGs met timeliness and quality goals defined by statute and internal IG policy. Specifically, we assessed the timeliness of DOD Hotline referrals and completion reports against its internal goals, along with DODIG senior official misconduct and whistleblower reprisal intakes, investigations, and oversight reviews against internal and statutory goals. We also assessed the timeliness of military service IG senior official and reprisal notifications, intakes, and investigations against DOD and statutory goals, and reviewed the results of DODIG quality assessments for DOD Hotline referrals, military service investigations, and DODIG senior official and whistleblower reprisal investigations.

We assessed the reliability of DODIG and military service IG data by administering questionnaires, interviewing cognizant officials, and reviewing case management system documentation and quality assurance procedures. We also compared select electronic data to fiscal years 2013 through 2017 case file documentation associated with our review of case files to determine whether dates had been properly recorded in the system. We determined that these data were sufficiently reliable for our purposes.

To identify factors affecting timeliness and quality, we interviewed IG officials and reviewed relevant documentation including strategic plans, briefing materials, and semiannual reports to Congress. We also compared DODIG and military service IG completed and planned efforts to improve timeliness and quality against Council of the Inspectors General on Integrity and Efficiency (CIGIE) standards for federal IGs¹ related to establishing performance plans with goals and performance

¹ See CIGIE *Quality Standards for Federal Offices of Inspector General* (August 2012).

measures, and *Standards for Internal Control in the Federal Government* related to assessing performance and improving performance.²

To determine the extent to which DODIG and the military service IGs have established processes to protect the confidentiality of whistleblowers, we assessed DOD and military service IG policies and procedures for handling whistleblower allegations against DOD policy, CIGIE standards for federal IGs,³ and statutory protections related to safeguarding whistleblower confidentiality.⁴ We also reviewed the results of DODIG's quality assurance reviews of the Air Force (2017), Army (2018), and Naval (2016) IGs. We performed a web-based survey of the entire population of 108 DODIG Administrative Investigations directorate employees directly involved with the handling of whistleblower cases to ascertain whether, in their view, confidentiality processes are being implemented in accordance with guidance and standards, identify potential confidentiality violations, and to gather perceptions on the integrity of the internal process for reporting misconduct, among other things. We removed four employees from our initial population of 112 employees because two employees left DODIG prior to the initiation of our survey and two employees were new to the organization and therefore likely not familiar with the issues covered by the survey.

To conduct the survey, we developed 27 questions covering (1) access to and protection of sensitive and classified whistleblower information; (2) confidentiality guidance, safeguards and identity disclosures; (3) resolving internal conflict through DODIG's Office of the Ombuds; and (4) reporting misconduct through the internal DODIG process for DODIG employees to

² GAO, *Standards for Internal Control in the Federal Government*, [GAO-14-704G](#) (Washington, D.C.: September 2014).

³ CIGIE was statutorily established as an independent entity within the executive branch by the *Inspector General Reform Act of 2008*, Pub. L. No. 110-409 (2008) and codified at 5 U.S.C. Appendix. Primarily comprised of inspectors general, CIGIE's mission is to address integrity, economy, and effectiveness issues that transcend individual government agencies and develop policies, standards, and approaches to aid in the establishment of a professional, well-trained, and highly skilled workforce in the offices of IGs. See CIGIE, *Quality Standards for Federal Offices of Inspector General* (August 2012) and *Quality Standards for Investigations* (Nov. 15, 2011).

⁴ See the Inspector General Act of 1978, as amended, which states that IGs shall not, after the receipt of a complaint or information from an employee, disclose the identity of the employee without the consent of the employee, unless the IG determines such disclosure is unavoidable during the course of the investigation. See 5 U.S.C., Appendix § 7(b).

report misconduct. A survey specialist helped to develop these questions, and another survey specialist provided independent feedback on the questions to ensure that content necessary to understand the questions was included and that the questions could be answered accurately and completely. To minimize errors that might occur from respondents interpreting our questions differently than we intended, we pretested our survey with seven DODIG employees to ensure the clarity and reasonableness of the questions.⁵ During the pretests, conducted in person and by phone, DODIG employees read the instructions and each question out loud and told us whether (1) the instructions and questions were clear and unambiguous, (2) the terms we used were accurate, and (3) they could offer a potential solution to any problems identified. We also asked them for a mock answer to ensure that the questions were understood as intended. We noted any potential problems identified by the reviewers and through the pretests and modified the questionnaire based on the feedback received. A full listing of survey questions is provided in appendix IV.

We conducted the survey between June 14, 2018, and July 6, 2018. To maximize our response rate, we sent reminder emails and contacted non-respondents by telephone to encourage them to complete the survey. In total, we received responses from 86 DODIG employees, achieving a response rate of 80 percent. Although not required, we assessed the potential for non-response bias by analyzing differences in the percent of DODIG employees per directorate and job position (e.g., investigator) that responded to our survey and the percent of potential DODIG respondents in each directorate and position. We found no meaningful differences between respondents and our population of potential respondents, indicating no evidence for non-response bias.⁶ Also, we took steps in the development of the survey, data collection, and data analysis to minimize nonsampling errors and help ensure the accuracy of the answers that were obtained.⁷ For example, a social-science survey specialist helped to

⁵ The pretests were conducted with one investigative support specialist, one investigator, two senior investigators, and three supervisory investigators.

⁶ All respondents to the survey answered two of the four most-sensitive survey questions, and no more than two did not respond to the other two questions.

⁷ The practical difficulties of administering any survey may introduce errors, commonly referred to as nonsampling errors. For example, differences in how a particular question is interpreted, the sources of information available to respondents, how the responses were processed and analyzed, or the types of people who do not respond can influence the accuracy of the survey results.

design the questionnaire, in collaboration with analysts having subject-matter expertise. Then, as noted earlier, the draft questionnaire was pretested to ensure that questions were relevant, clearly stated, and easy to comprehend, and it was also reviewed by another specialist with expertise in survey development.

We calculated the frequency of responses to our closed-ended survey questions and performed content analysis on the open-ended questions to identify common themes from across the responses and to determine their frequencies. The quantitative analysis was performed by one analyst and independently reviewed by another analyst. For the qualitative analysis, a standard coding scheme was developed to identify common themes and determine their frequencies. We also used professional judgment to identify other themes that were determined to be important based on our review of case files, discussions with DODIG management, and review of guidance and relevant standards.

To determine the extent to which DODIG and the military service IGs are able to access and safeguard classified and sensitive information necessary to handle whistleblower complaints, we reviewed documentation and interviewed officials on the extent to which DODIG and the military service IGs have developed, implemented, and assessed key information technology (IT) security controls, and authorized the systems and applications used to process, store, and transmit sensitive whistleblower information per requirements and standards prescribed by DOD,⁸ the Office of Management and Budget,⁹ and the National Institute of Standards and Technology.¹⁰ Collectively, these documents delineate an array of documentary and procedural requirements related to the assessment of IT security controls and the authorization to operate IT systems and applications. We also reviewed plans and interviewed

⁸ DOD Instruction 8510.01, *Risk Management Framework for DOD Information Technology* (Mar. 12, 2014) (Incorporating Change 2, Jul. 28, 2017).

⁹ Office of Management and Budget, Circular No. A-130, *Managing Federal Information as a Strategic Resource* (Jul. 28, 2016).

¹⁰ See National Institute of Standards and Technology, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans*, Special Publication 800-53A, Revision 4 (December 2014); *Security and Privacy Controls for Federal Information Systems and Organizations*, Special Publication 800-53, Revision 4 (April 2013); and *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, SP 800-37, Revision 1 (February 2010).

cognizant officials on the development and implementation of the Defense Case Activity Tracking System enterprise (D-CATSe)—DOD’s future system for managing whistleblower information across DODIG and the military service IGs, and reviewed DODIG’s quality assurance reviews of the Air Force (2017), Army (2018), and Naval IGs (2016). Separately, we reviewed data and information on the number and percentage of DODIG and military service IG classified cases¹¹ closed in fiscal year 2017, the number and allocation of DODIG and military service IG staff possessing security clearances, and the processes and procedures for storing and accessing classified information within DODIG and the military service IGs against DOD policy related to establishing controls to ensure access to classified information is limited to authorized persons.¹² We assessed the reliability of classified case data by administering questionnaires to cognizant officials, and determined the data were sufficiently reliable for the purpose of reporting the number of classified cases closed in fiscal year 2017.

To determine the extent of substantiated and potential confidentiality violations and retaliatory investigations involving DODIG employees, we obtained and analyzed available fiscal year 2013 through 2018 data on known or perceived violations of confidentiality standards and retaliatory investigations from DODIG and the military service IGs. We selected data covering this period of time because they constituted the most recent and reliable data available, and because DODIG officials told us that data prior to fiscal year 2013 were unreliable. We also reviewed fiscal year 2013–2018 complaint data from the Office of Special Counsel¹³ and the CIGIE Integrity Committee in order to identify possible violations of confidentiality standards or retaliatory investigations.¹⁴ We assessed the reliability of DODIG and service IG data by administering questionnaires, interviewing cognizant officials, and reviewing the methods used to query

¹¹ For the purposes of this report, a classified case refers to a case or allegation including classified information.

¹² DOD Manual 5200.01 Vol.3, *DOD Information Security Program: Protection of Classified Information* (Feb. 24, 2012) (Incorporating change 2, Mar. 19, 2013).

¹³ The Office of Special Counsel is an independent agency established under the Whistleblower Protection Act of 1989 to investigate whistleblower reprisal and other federal personnel action complaints.

¹⁴ The CIGIE Integrity Committee receives, reviews, and refers for investigation whistleblower complaints made against inspectors general, designated staff members of an IG, and the Special Counsel and Deputy Special Counsel of the Office of Special Counsel.

IG case management systems for this information. We determined the data to be sufficiently reliable for the limited purpose of identifying potential confidentiality violations and retaliatory investigations.

To evaluate the extent to which select misconduct and reprisal cases involving civilian DOD Presidential appointee with Senate confirmation (PAS) officials met key documentation and reporting requirements, we reviewed all 125 administrative misconduct and reprisal cases involving Senate-confirmed civilian official subjects that were dismissed by DODIG in fiscal years 2013 through 2017. We chose to review cases from this period because they constituted the most recent and complete data in DODIG’s case management system and would therefore most accurately reflect the extent to which the majority of DODIG’s cases included required documentation. Also, DODIG officials informed us that information on cases prior to the implementation of the current case management system in fiscal year 2013 were both incomplete and unreliable. During the course of our review, we removed five out-of-scope cases from the original population of 130 cases, reducing the number of cases in our population from 130 to 125. Four cases were removed because the related allegations were investigated, and one case was removed because it was a record used to track an investigation occurring at a military service IG. Table 8 shows the distribution per fiscal year of closed misconduct and reprisal cases involving civilian DOD PAS subjects by the result of the case.

Table 8: Distribution of Dismissed Cases Involving Civilian DOD Presidential Appointees with Senate Confirmation, Fiscal Years 2013-2017

Case Type	Fiscal year 2013	Fiscal year 2014	Fiscal year 2015	Fiscal year 2016	Fiscal year 2017
Misconduct	17	28	17	36	19
Reprisal	0	3	0	2	3
Total	17	31	17	38	22

Source: GAO analysis of Department of Defense Inspector General (DODIG) data. | GAO-19-198

To conduct the case-file review, we developed and used a data collection instrument to guide our review regarding general case characteristics and the presence of information and documentation required by DOD policies¹⁵ and CIGIE best practices.¹⁶ Core elements of this instrument

¹⁵ Such as Department of Defense Office of Inspector General, *AI Investigations Manual* (Mar. 29, 2016).

¹⁶ CIGIE, *Quality Standards for Investigations* (November 2011).

were shared with DODIG officials to ensure the instrument aligned with the policies and practices in place when the cases were dismissed. These core elements represented individual documents and data elements. We incorporated DODIG's feedback into our instrument before commencing the file review. Examples of elements in our review that represent key data in DODIG's database or constitute documentation of key steps of the case-handling process include the following:

- case open date,
- case close date,
- protected disclosures,
- personnel actions,
- incoming complaints,
- disposition of the matter at intake,
- dismissal approval,
- required notifications, and
- dismissal rationale.

To validate the data collection instrument and ensure consistency in its application, we developed and followed standard procedures to review a test sample of 11 case files that were selected from each stratum of cases (e.g., misconduct) to ensure that each case type was tested at least once. In reviewing the sample, we adjusted the relevant case file elements for each case based on its type and circumstances and captured responses in our data collection instrument accordingly. To help ensure the accuracy of the information we collected, one analyst reviewed each casefile and coded for the presence of required information using the data collection instrument, and another analyst reviewed the first analyst's work. In the event that disagreement between the two analysts occurred, the analysts discussed and resolved the disagreement by identifying and reviewing supporting database information or documentation, and obtaining the input of a third analyst, if necessary, until a final resolution was made. We reviewed all cases dismissed during this period; for this reason, the results of this analysis do not have a sampling error.

To identify other characteristics of DODIG cases involving civilian DOD PAS officials, we also analyzed fiscal years 2013-2017 case data to determine the number of cases closed by fiscal year, case types, case

dispositions, source organizations, and the frequency and type of alleged misconduct. Separately, we also reviewed documentation from DODIG on civilian DOD PAS official allegations and investigation results reported to the Secretary of Defense and Congress since fiscal year 2013.

In addressing our objectives, we met with officials from the organizations identified in table 9.

Table 9: Organizations Contacted by GAO

Department of Defense	Department of Defense Office of Inspector General	Administrative Investigations Directorate
		DOD Hotline
		Defense Case Activity Tracking System Program Management Office
		Investigations of Senior Officials Directorate
		Office of the Chief Information Officer
		Office of General Counsel
		Office of the Ombuds
		Office of Professional Responsibility
		Whistleblower Protection Ombudsman
		Whistleblower Reprisal Investigations Directorate
		Standards of Conduct Office
		Complaints Resolution Directorate
		Senior Officials Directorate
Air Force Office of Inspector General	Assistance Division	
	Investigations Division	
Army Office of Inspector General	Assistance & Investigations Division	
	Inspections Division	
Marine Corps Office of Inspector General	Information Technology Program Manager	
	Military Whistleblower Reprisal Branch	
	Special Inquiries Division	
Other Organizations	U.S. Office of Special Counsel	
	Council of the Inspectors General on Integrity and Efficiency	Integrity Committee
	Human Rights Watch	
	Government Accountability Project	

Source: GAO | GAO-19-198

We conducted this performance audit from October 2016 to March 2019 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain

sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

While this audit was initiated in October 2016, work was suspended from December 2016 until September 2017 due to other engagement work.

Appendix II: Additional Examples of DODIG Initiatives to Improve Timeliness

This appendix provides additional examples of Department of Defense Office of Inspector General (DODIG) timeliness improvement initiatives. According to DODIG officials, recent steps to improve the timeliness of whistleblower reprisal and senior official misconduct intakes, investigations, and oversight reviews include:

- Transferring the intake of most military reprisal complaints to the DODIG oversight branch for increased consistency.
- Changing the intake metric from 30 to 45 days for non-military reprisal cases to allow for more robust intakes.
- Not requiring a clarification interview when a written reprisal complaint is clear.
- Requesting documents from the employer at the intake stage in contractor reprisal cases.
- Interviewing subjects early in the investigation, when appropriate.
- Conducting investigative travel only when doing so would save time or for other compelling reasons. Otherwise, most interviews are conducted by phone or video teleconference and information is requested in opening letters for investigations to facilitate early receipt of documentary evidence.
- Using summary reports of investigation to facilitate timelier report-writing and review. DODIG issued 24 summary reports in fiscal year 2018, starting in May, for simple, non-substantiated investigations.
- Eliminating the requirement to conduct peer reviews of the reprisal reports of investigation, except at supervisors' discretion.
- Using standardized complaint notification and determination forms across DOD to formalize the processing of complaints received by component and service IGs.
- Implementing a more robust intake process for senior official misconduct investigations, which includes complaint clarifications and more investigative work. According to DODIG officials, most of the complaints reviewed during this new process would have otherwise been investigated by DODIG or the military service IGs, with a negative impact on the overall timeliness of investigations.
- Authorizing the military service IGs to close and simultaneously notify the DODIG reprisal investigations directorate of actions taken for complaints relating to uncooperative complainants, untimely

complaints, and withdrawn complaints. This has increased notification rates and decreased processing time, according to DODIG officials.

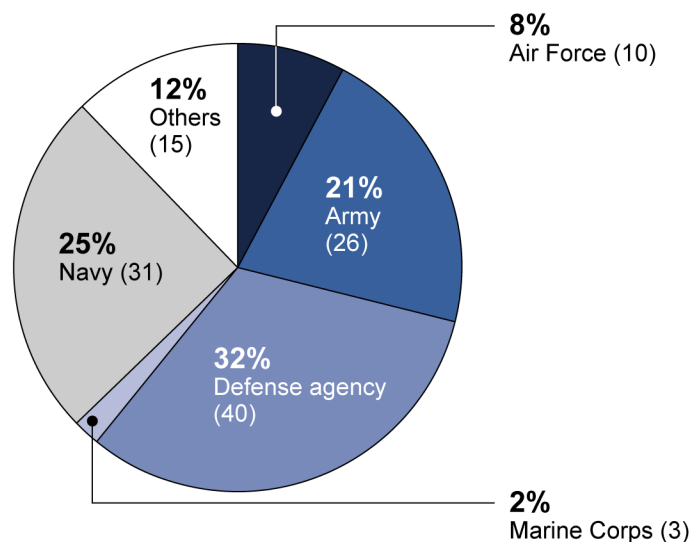
Appendix III: Characteristics of Closed Misconduct and Reprisal Cases Involving Civilian DOD Presidential Appointees with Senate Confirmation

This appendix provides information on the characteristics of closed and dismissed misconduct and reprisal cases involving civilian DOD Presidential appointee with Senate confirmation (PAS) officials based on our analysis of fiscal year 2013 through fiscal year 2017 case data from the Department of Defense Office of Inspector General (DODIG) case-management system and our review of dismissed cases. DODIG closed 129 cases from October 1, 2012, through September 30, 2017, of which 125 were dismissed. Of the 125 dismissed cases, 117 were misconduct cases and eight were reprisal cases.

Organizational Source of Complaints Dismissed in Fiscal Years 2013-2017

DODIG dismissed 125 civilian DOD PAS official misconduct and reprisal cases. The largest number of cases—40 (32 percent)—were submitted by defense agency employees. Employees from the Navy submitted the next highest number of complaints, with 31 (25 percent), followed by the Army, which accounted for 26 (21 percent) of the complaints. Figure 9 shows the percentage of dismissed cases closed from fiscal years 2013 through 2017, by organizational source.

Figure 9: DODIG Dismissed Misconduct and Reprisal Cases Involving Civilian DOD Presidential Appointees with Senate Confirmation, by Organizational Source, Fiscal Years 2013-2017



Source: GAO analysis of the Department of Defense Office of Inspector General (DODIG) data. | GAO-19-198

DODIG Number of Days to Close Dismissed Cases, Fiscal Years 2013-2017

Our review of the 125 dismissed civilian DOD PAS official cases closed by DODIG from fiscal years 2013 through 2017 showed that the majority of cases were closed in 30 days or less. Specifically, approximately 81 percent of the cases were closed in 30 days or less, and 58 percent of the cases were closed in 10 days or less. Table 10 groups the cases dismissed in each fiscal year from fiscal years 2013 through 2017 by the number of days to close.

Table 10: DODIG Dismissed Misconduct and Reprisal Cases Involving Civilian DOD Presidential Appointees with Senate Confirmation, by Number of Days to Close and Percentage, Fiscal Years 2013-2017

Days to close	Case type		
	Senior officials	reprisal	Percentage of total
10 or less	71	1	58 percent
30 or less	26	3	23 percent
60 or less	9	2	9 percent
90 or less	5	1	5 percent
Over 90	6	1	6 percent

Source: GAO analysis of Department of Defense Office of Inspector General (DODIG) data. | GAO-19-198

Notes: Percentages do not equal 100 due to rounding.

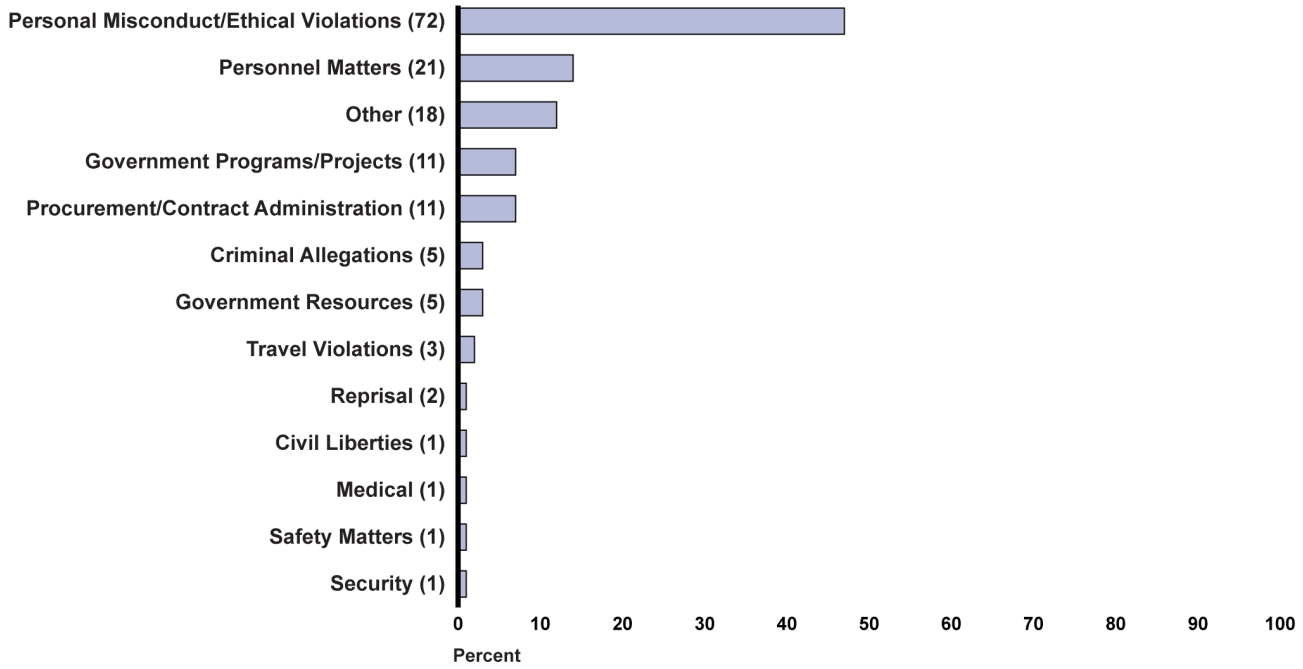
DODIG has an internal goal to complete military reprisal intake reviews within 30 days, civilian and contractor reprisal reviews within 45 days, and senior official misconduct intake reviews within 15 days.

DODIG Closed Misconduct Case Allegations, Fiscal Years 2013-2017

We reviewed data on the number and type of allegations made against civilian DOD PAS officials in the 117 closed misconduct cases from fiscal years 2013 through 2017. In total, there were 152 allegations across the 117 closed cases. Allegations are grouped into 13 broad categories and 38 sub-allegation categories. From fiscal years 2013 through 2017, we found that the greatest proportion of allegations, at 47 percent, were personal misconduct and ethical violations. Personnel matters—at 14 percent—and “other”—an indeterminate category at 12 percent—were the next two largest in proportion of allegations. Figure 10 provides the percentages of allegations in closed misconduct cases from fiscal years 2013 through 2017.

Appendix III: Characteristics of Closed
 Misconduct and Reprisal Cases Involving
 Civilian DOD Presidential Appointees with
 Senate Confirmation

Figure 10: DODIG Closed Misconduct Case Allegations Involving Civilian DOD Presidential Appointees with Senate Confirmation, by Percentage, Fiscal Years 2013-2017



Source: GAO analysis of the Department of Defense Office of Inspector General (DODIG) data. | GAO-19-198

Note: Each allegation includes at least one sub-allegation.

Appendix IV: Survey of Select DODIG Employees

GAO administered the survey questions shown in this appendix to learn more about DODIG processes related to the access and protection of whistleblower records, and the avenues available to DODIG employees to resolve conflict and report alleged misconduct themselves. The survey was divided into four sections: information access and protection, confidentiality, resolving internal conflict, and reporting misconduct. Survey questions without response options were open-ended. This appendix accurately shows the content of the web-based survey but the format of the questions and responses options have been changed for readability in this report. For more information about our methodology for designing and administering the survey, see appendix I.

1. How long have you worked in Administrative Investigations (AI)? Please consider your full tenure across all AI directorates (DOD Hotline, Investigations of Senior Officials, and Whistleblower Reprisal Investigations) if you have worked in more than one directorate. (Response options provided: radio buttons labeled “Less than 1 year,” “1 year or more but less than 5 years,” “5 years or more but less than 10 years,” and “10 years or more.”)

SECTION I: Information Access and Protection

2. In your current position, are you generally able to access all types of unclassified information necessary to perform the duties required of your position? This could include access to documentary evidence or witnesses, among other information.
 - Yes → SKIP to Question 3
 - No → Continue to i
 - i. Please describe any obstacles that impede your ability to access all types of unclassified information necessary to perform the duties required in your position.
3. Have you been provided guidance that specifies requirements for ensuring that whistleblower records are properly secured, both physically and electronically? For the purposes of this survey, *whistleblower records are not specific to reprisal*, but encompass all contacts, complaints, allegations, cases, and investigations related to possible violations of law, rules, or regulations; mismanagement; gross waste of funds; abuse of authority; reprisal; or substantial and specific danger to public health and safety. Guidance can include but

may not be limited to documents, training, emails, or in-person discussions/briefings.

- Yes → Continue to i
- No → SKIP to iii

i. Have you received any of the following types of guidance that specifies requirements for properly securing whistleblower records? Select one from each row

	Yes	No	I don't know
Formal training (in-person/w eb-based)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Informal training (staff meetings/briefings)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Direction from supervisor	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Written policy/procedure	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Other	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Please describe any other guidance you have received .			

} Continue to ii

ii. Do you believe the guidance identified above is sufficient or insufficient in specifying requirements for properly securing whistleblower records in your directorate? *Select only one*

- Sufficient → SKIP to Question 4
- Insufficient → Continue to 1 below
- Not sure → SKIP to Question 4

1. Why do you believe the guidance is insufficient? SKIP to Question 4

iii. Would guidance that specifies access restrictions and security controls for handling whistleblower records be helpful? (Response options provided: radio button labeled “yes” and “no.”)

1. Please explain why guidance would or would not be helpful.

4. Are you aware of any controls in place to restrict access to D-CATS records to only DODIG employees (either within or outside your directorate) with a need to know? Select only one

- Yes → Continue to i
 - No → SKIP to Question 5
 - I'm not sure → SKIP to Question 5
 - i. Please describe the control(s) in place to restrict access to D-CATS records.
5. During your tenure at DODIG, have you or other DODIG employees (either within or outside your directorate) been able to access records in D-CATS without a need to know? This applies to potential access to records, regardless of whether anyone actually accessed records or not.
- Yes → Continue to i
 - No → SKIP to Question 6
 - I don't know → SKIP to Question 6
 - i. Which DODIG directorate's records have you or other DODIG employees been able to access without a need to know? (Response options provided: checkboxes labeled "DOD Hotline," "Investigations of Senior Officials," "Whistleblower Reprisal Investigations," and "Office of Professional Responsibility.")
 - ii. Are you aware of any actions taken to address the ability of DODIG employees to access records without a need to know? Examples of actions taken include a policy or procedure change, additional guidance, or other actions taken.
 - Yes → Continue to 1 below
 - No → SKIP to 2 below
 - 1. Please describe the action(s) taken.
 - 2. What improvements, if any, could be made to address the ability of DODIG employees to access records without a need to know?
6. Do you believe protections are sufficient or insufficient to ensure only DODIG employees with a need to know can access records in D-CATS? Select only one
- Sufficient → Continue to i

-
- Insufficient → Continue to i
 - Not sure → SKIP to Question 7
 - i. Why do you believe the protections are sufficient or insufficient?
7. Are you able to access classified information when needed to perform the duties required of your position? Select only one
- Yes → SKIP to Question 8
 - No → Continue to i
 - I do not require access to classified information to perform the duties of my position → SKIP to Question 8
 - i. Please describe any current obstacles to accessing classified information necessary to perform the duties required of your position.
8. Do you believe protections that are in place in your directorate are sufficient or insufficient to ensure that only those people with a need to know handle classified whistleblower records? Select only one
- Sufficient → Continue to i
 - Insufficient → Continue to i
 - Not sure → SKIP to the next section
 - i. Why do you believe the protections are sufficient or insufficient?

SECTION II: Confidentiality

9. Have you been provided guidance that describes how to maintain the confidentiality of all individuals (both known and confidential complainants, witnesses and subjects) involved in the whistleblower records you handle? Guidance can include but may not be limited to documents, training, emails, or in-person discussions/briefings.
- Yes → Continue to i
 - No → SKIP to iii
 - i. Have you received any of the following types of guidance that describes how to maintain the confidentiality of all individuals (both known and confidential complainants, witnesses and

subjects) involved in the whistleblower records you handle?
Select one from each row

	Yes	No	I don't know
Formal training (in-person/w eb-based)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Informal training (staff meetings/briefings)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Direction from supervisor	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Written policy/procedure	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Other	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Please describe any other guidance you have received.			

} Continue to ii

ii. Do you believe the guidance identified above is sufficient or insufficient in specifying how to maintain the confidentiality of all individuals (both known and confidential complainants, witnesses and subjects) involved in the whistleblower records you handle?

- Sufficient → SKIP to Question 10
- Insufficient → Continue to 1 below
- Not sure → SKIP to Question 10

1. Why do you believe the guidance is insufficient? (After answering, SKIP to Question 10)

iii. Would guidance that describes how to maintain the confidentiality of all individuals (both known and confidential complainants, witnesses and subjects) involved in the whistleblower records you handle be helpful?

- Yes → Continue to 1
- No → Continue to 1

1. Please explain why guidance would or would not be helpful.

10. To your knowledge, what safeguards, if any, are in place within your directorate to protect the identities of individuals (both known and confidential complainants, witnesses and subjects) involved in whistleblower records? Safeguards may include but are not limited to database restrictions and protocols for sharing information.

11. Have you been provided guidance that specifies how to determine whether disclosing the identity of a complainant or source (e.g., witness) is unavoidable? Guidance can include but may not be limited to documents, training, emails, or in-person discussions/briefings.

- Yes → Continue to i
- No → SKIP to iii

i. Have you received any of the following types of guidance that specifies how to determine whether disclosing the identity of a complainant or source (e.g., witness) is unavoidable? *Select one from each row*

	Yes	No	I don't know
Formal training (in-person/web-based)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Informal training (staff meetings/briefings)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Direction from supervisor	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Written policy/procedure	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Other	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

} Continue to ii

Please describe any other guidance you have received.

ii. Do you believe the guidance identified above is sufficient or insufficient in specifying how to determine whether disclosing the identity of a complainant or source (e.g., witness) is unavoidable?

- Sufficient → SKIP to 2 below
- Insufficient → Continue to 1 below
- Not sure → SKIP to 2 below

1. Why do you believe the guidance is insufficient?
2. What improvements, if any, do you think could be made to guidance specifying how to determine whether disclosing the identity of a complainant or source (e.g., witness) is unavoidable? (After answering, SKIP to Question 12)

-
- iii. Would guidance that specifies how to determine whether disclosing the identity of a complainant or source (e.g., witness) is unavoidable be helpful? (Response options provided: radio buttons labeled “yes” and “no.”)
1. Please explain why guidance would or would not be helpful.
12. To your knowledge, is there one or more official(s) who is responsible for determining whether disclosing the identity of a complainant or source (e.g., witness) is unavoidable?
- Yes → Continue to i
 - No → SKIP to Question 13
 - I don't know → SKIP to Question 13
- i. Who is responsible for determining whether disclosing the identity of a complainant or source (e.g., witness) is unavoidable?
13. While working in AI, have you ever encountered a situation where disclosing the identity of a complainant or source (e.g., witness) was unavoidable?
- Yes → Continue to i
 - No → SKIP to Question 14
- i. Please describe the general circumstance(s) and the steps you took to verify that the circumstance(s) required disclosing the identity of a complainant or source (e.g., witness). Please do not provide individual names related to the actors involved.
14. Between June 1, 2017, and today, are you aware — either by experiencing firsthand or directly observing actions of another person — of an instance where the identity of a complainant or source (e.g., witness) was disclosed by a DODIG employee to an organization or individual without a need to know (i.e., an avoidable disclosure)? Please check only one below.
- No, I am not aware of any avoidable disclosures → SKIP to Question 15
 - Yes, I am aware of one or more avoidable disclosure(s) → Continue to i

- i. How many avoidable disclosures are you aware of between June 1, 2017, and today? For example, if the identity of a complainant was revealed to one person who did not have a need to know, please consider that event as one instance. Similarly, if the identity of a source was revealed separately to two different people who did not have a need to know, please consider those events as two instances.
 - ii. Please describe any actions taken in response to the avoidable disclosure(s) you are aware of between June 1, 2017, and today. Examples of actions taken include but may not be limited to retracting/recalling a referred complaint, a change to policy, procedure or guidance, and notifying the complainant or source, among other actions.
15. What improvements, if any, could be made to prevent avoidable disclosures from happening in the future?
16. Please describe any best practices that you follow to help prevent avoidable disclosures.

SECTION III: Resolving Internal Conflict

17. Have you ever contacted the DODIG Office of the Ombuds or participated in a DODIG Office of the Ombuds activity in order to address conflict among DODIG employees? Examples of DODIG Office of the Ombuds activities include but are not limited to providing confidential advice for resolving conflict among peers and supervisors and participating in an Ombuds-led mediation among DODIG employees.
- Yes → Continue to i
 - No, but I know about the DODIG Office of the Ombuds → SKIP to Question 18
 - I do not know about the DODIG Office of the Ombuds → SKIP to the next section
- i. Do you believe the DODIG Office of the Ombuds provided or is providing sufficient or insufficient assistance to address the conflict(s) for which you contacted the Ombuds or participated in an Ombuds activity?
- Sufficient → Continue to 1

- Insufficient → Continue to 1
- Too soon to tell → Continue to 1

1. Please describe, in general terms, your latest experience working with the DODIG Office of the Ombuds. Please do not provide the names of individuals involved with your experience.

18. Have you ever considered reaching out to the DODIG Office of the Ombuds, but ultimately chose not to?

- Yes → Continue to i
- No → SKIP to the next section

i. How much, if at all, did each of the following contribute to your decision not to utilize DODIG Office of the Ombuds services? *Select one in each row.*

	Not at All	Slightly	Somew hat	Very Much	Don't Recall
Resolved the issue through another avenue	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Not sure how to initiate contact w ith the Ombuds	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Concern about length of process	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Concern about objectivity or conflict of interest w ithin the Office of the Ombuds	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Fear that confidentiality w ould be compromised	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Fear of retaliation or reprisal from w ithin DODIG	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Other	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Please describe any other factor(s) that contributed to your decision not to utilize DODIG Office of the Ombuds services.					

SECTION IV: Reporting Misconduct

19. As a DODIG employee, have you ever personally reported misconduct against another DODIG employee through DODIG's

internal process for investigating alleged misconduct? For the purposes of this survey, “misconduct” refers to (1) a violation of a provision of criminal law, (2) a violation of a recognized standard, such as a federal or DOD regulation, or (3) a matter of concern involving DOD leadership that could reasonably be expected to be of significance to DODIG.

- Yes → Continue to i
- No → SKIP to iii

i. Did you report misconduct on or before September 30, 2016?

- Yes → Continue to 1 below
- No → SKIP to ii

1. Do you believe your report(s) of misconduct on or before September 30, 2016 were investigated in a fair and objective manner? (Response options provided: radio buttons labeled “yes” and “no.”)

a. Please describe your general experience(s) in reporting misconduct against a DODIG employee on or before September 30, 2016, including why you do or do not believe your report(s) of misconduct were investigated in a fair and objective manner. Please do not provide the names of individuals related to the misconduct you reported.

ii. Did you report misconduct on or after October 1, 2016?

- Yes → Continue to 1 below
- No → SKIP to Question 20

1. Do you believe your report(s) of misconduct on or after October 1, 2016 were investigated in a fair and objective manner? (Response options provided: radio buttons labeled “yes,” “no,” and “too early to have an opinion”)

a. Please describe your general experience(s) in reporting misconduct against a DODIG employee on or after October 1, 2016, including why you do or do not believe your report(s) of misconduct were investigated

in a fair and objective manner. Please do not provide the names of individuals related to the misconduct you reported.

iii. Do you know how to report misconduct against another DODIG employee through DODIG’s internal process? (Response options provided: radio buttons labeled “yes” and “no.”)

20. Thinking about the time period on or before September 30, 2016, did you ever consider reporting misconduct against a DODIG employee through DODIG’s internal process, but ultimately *choose not to*?

- Yes → Continue to i
- No → SKIP to Question 21

i. How much, if at all, did each of the following contribute to your decision not to report incident(s) of misconduct on or before September 30, 2016? *Select one in each row.*

	Not at All	Slightly	Somewhat	Very Much	Don't Recall
Resolved the issue through another avenue	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Not sure how to report misconduct	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Concern about length of process	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Concern about objectivity or conflict of interest within DODIG’s internal process to report misconduct	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Fear that confidentiality would be compromised	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Fear of retaliation or reprisal from within DODIG	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Other	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Please describe any other factor(s) that contributed to your decision not to report incidents of misconduct on or before September 30, 2016.					

21. Thinking about the time period on or after October 1, 2016, did you ever consider reporting misconduct against a DODIG employee through DODIG’s internal process, but ultimately choose not to?

- Yes → Continue to i below
- No → SKIP to Question 22

i. How much, if at all, did each of the following contribute to your decision not to report incident(s) of misconduct on or after October 1, 2016? *Select one in each row.*

	Not at All	Slightly	Somewhat	Very Much	Don't Recall
Resolved the issue through another avenue	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Not sure how to report misconduct	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Concern about length of process	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Concern about objectivity or conflict of interest within DODIG's internal process to report misconduct	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Fear that confidentiality would be compromised	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Fear of retaliation or reprisal from within DODIG	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Other	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Please describe any other factor(s) that contributed to your decision not to report incidents of misconduct on or after October 1, 2016.					

22. How well, if at all, do you believe DODIG's internal process for reporting misconduct protects the confidentiality of DODIG employees? (Response options provided: radio buttons labeled "Not at all," "Slightly," "Somewhat," "Very well," and "I don't know.")
23. What improvements, if any, do you think could be made to DODIG's internal process for reporting misconduct to protect the confidentiality of DODIG employees?
24. How well, if at all, do you believe DODIG's internal process handles misconduct allegations against DODIG employees? This includes activities associated with both assessing incoming complaints and subsequently investigating them, as appropriate. (Response options provided: radio buttons labeled "Not at all," "Slightly," "Somewhat," "Very well," and "I don't know.")

-
25. What factors contribute to your opinion about DODIG's internal process for handling misconduct allegations against DODIG employees?
 26. What improvements, if any, do you think could be made to DODIG's internal process to improve the handling of misconduct allegations?
 27. If you would like to comment on any of the topics covered by this survey, or anything else that you feel might be relevant to our review on the DOD whistleblower program, please do so below.

Appendix V: Comments from the Department of Defense



INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
4800 MARK CENTER DRIVE
ALEXANDRIA, VIRGINIA 22350-1500

FEB 19 2019

Ms. Cathleen A. Berrick, Managing Director
Defense Capabilities and Management
U.S. Government Accountability Office
441 G. Street, N.W.
Washington, DC 20548

Dear Ms. Berrick,

This is the DoD Office of Inspector General's (DoD OIG) response to the GAO's report, "Whistleblower Protection: Analysis of DoD's Actions to Improve Case Timeliness and Safeguard Confidentiality (GAO 19-128)."

We appreciate the GAO's careful review of the Department of Defense's whistleblower protection program and its professional communications with the DoD OIG and the offices of the military service Inspectors General (IGs).

We value the GAO's oversight, and we believe that this report, and its recommendations, will help further improve whistleblower reprisal investigations by the DoD OIG and the military service IGs. As noted below, we concur with the report's recommendations and will seek to implement them. Additionally, the military service IGs concur with the report's recommendations. We have enclosed their responses as exhibits to this letter.

We also appreciate this report's recognition of the many improvements that we have been making in the timeliness of intake reviews, investigations, and oversights, as well as the safeguarding of whistleblower information and confidentiality. For example, the report noted that the DoD OIG met its timeliness goals for civilian and contractor case intakes and for senior official misconduct oversight reviews, despite the 98 percent increase in whistleblower reprisal complaints over the past 5 years. (See page 13 of the GAO report.)

Further, the report noted that the DoD OIG completed a record number of 60 reprisal investigations in fiscal year 2018, compared to 37 investigations in fiscal year 2017. We have reduced the average case age of open and closed whistleblower reprisal investigations, and the average age of open investigations on December 1, 2018, was 284 days, compared to 370 days in November 2018. In addition, the average age of the DoD OIG's reprisal investigations has continued to improve since the GAO's draft report was issued. On January 31, 2019, the average age of open investigations was 215 days. We will continue to focus on this issue and expect that the average age of open cases will continue to decline.

The report noted that the DoD OIG and the military service IGs met quality goals related to the thoroughness and completeness of senior official and whistleblower reprisal investigations. (See page 17 of the GAO report.) The report further noted that the DoD Hotline met quality goals for thoroughness of complaint referrals in 97 percent of the assessment criteria evaluated

This letter relates to GAO-19-198.

See page 15.

See pages 20-21 for DODIG quality goals. See pages 25-26 for military service IG quality goals.

See page 21.

by the GAO, and 100 percent of the DoD OIG's reprisal investigations complied with quality goals for thoroughness and documentation. (See pages 18-19 of the GAO report.)

See pages 50-53.

The report also noted that the DoD OIG case files for dismissed misconduct and reprisal cases contained key documentation and data to demonstrate compliance with significant aspects of the case handling process. (See page 45 of the GAO report.)

See page 26.

The report acknowledged the important initiatives that the DoD OIG and Military Service IGs have implemented to improve timeliness. (See page 23 of the GAO report.) For example, the DoD OIG increased its staff to address the significant increase in DoD Hotline, senior official misconduct, and reprisal cases. Specifically, we increased from 114 in fiscal year 2016 to 147 full-time equivalents in fiscal year 2018, and are further increasing the staff assigned to these matters. Similarly, the Marine Corps IG hired an additional investigator, and the Army IG reassigned staff to improve its efforts in addressing the reprisal caseload.

The report also noted the DoD OIG's implementation of an alternative dispute resolution (ADR) process to mediate reprisal complaints. This program seeks to resolve many complaints with the voluntary agreement of the parties, avoiding lengthy investigations and providing relief for complainants quickly. In fact, the DoD OIG's ADR program was recently praised in the Project on Government Oversight's July 9, 2018, report, "THE WATCHDOGS AFTER FORTY YEARS: Recommendations for Our Nation's Federal Inspectors General." That report stated, "It can take years to resolve whistleblower reprisal claims, and, in the meantime, the whistleblower is often forced to wait with their life on hold. To increase efficiency, CIGIE [the Council of Inspectors General on Integrity and Efficiency] should assess the DoD IG's recent alternative dispute resolution initiative as a potential model for larger OIGs."¹

See page 29.

The GAO report noted that the DoD OIG has established policies and procedures to protect whistleblower confidentiality, including obtaining express whistleblower consent to disclose their identity outside the DoD Hotline on a need-to-know basis, and documenting the whistleblower's consent decision in the case record. The GAO also found that 80 percent of DoD OIG respondents to a GAO survey said guidance they receive on protecting confidentiality is sufficient to maintain confidentiality of individuals involved in OIG investigations. (See page 26 of the GAO report.)

See page 26.

We also appreciate the recognition of other DoD OIG ongoing initiatives in these and other areas. We believe that the initiatives referenced in GAO Table 3 (on page 23) and Appendix II of the report will further improve the timeliness of intakes, investigations, and oversights, while enhancing the quality of IG reports. Several of the more significant initiatives noted by the GAO include:

- Using summary reports of investigation for simple, non-substantiated investigations, to facilitate more timely investigations and issuance of reports.
- Implementing a more robust intake process for senior official misconduct investigations, including complaint clarification interviews, which has had a positive impact on the overall timeliness of investigations.

¹ https://docs.pogo.org/report/2018/2018-07-09_POGO_The_Watchdogs_After_40_Years_IG_Report.pdf?_ga=2.261802829.1385200566.1541546549-334568156.1508359103

- Establishing standardized complaint notification and determination forms across the DoD to formalize and make more efficient the processing of complaints received by component and military service IGs.
- Centralizing intake functions to shorten complaint review processes and enhance the consistency of intake evaluations.

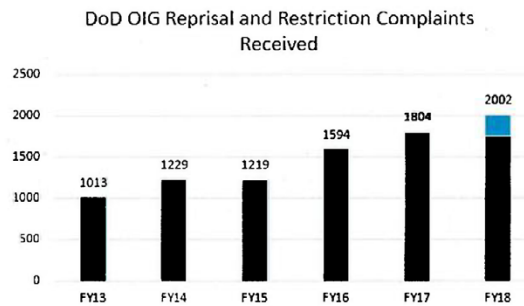
However, we recognize, and agree with the GAO, that more improvements can and should be made, and we will seek to implement the recommendations to continue the improvement process.

Finally, we believe it is important to note some areas in the report where the GAO's findings and statements warrant further context. We describe a few of these areas below.

Timeliness Issues

The report's findings concerning the DoD OIG's fiscal year 2018 timeliness goals present data in a manner that understates the DoD OIG's improvements in timeliness. For example, the report states that the DoD OIG did not meet timeliness goals related to average days of senior official and military reprisal intakes, and average days for reprisal oversight reviews. However, the statistics in Figure 2 show that the DoD OIG met its timeliness goals in more than 60 percent of all senior official and reprisal intake cases, including in 87 percent of senior official oversight review cases. Further, while the DoD OIG's average number of days for completing senior official intakes was 17 days -- against a goal of 15 days -- the DoD OIG met the 15-day goal in more than 70 percent of the 631 senior official intakes it concluded during the fiscal year.

We also appreciate the report's mention of the burgeoning whistleblower reprisal caseload. The GAO report states, on page 13, that the number of whistleblower reprisal cases increased from 1,013 to 2,002 over the past 5 years, and that in fiscal year 2018, the DoD Hotline received 12,470 complaints from potential whistleblowers. (See page 2 of the GAO report.) To better illustrate this point, the following chart shows the increase in reprisal and restriction complaints received since fiscal year 2013:



Confidentiality and Accessibility Issues

The report made several findings and recommendations concerning the existence and effectiveness of policy guidance for protecting the confidentiality of whistleblowers. We generally concur with those findings and recommendations. However, the report presented some information in a manner that could create an incomplete impression of the DoD OIG's commitment to protecting whistleblower confidentiality.

For example, the report presented survey data on some DoD OIG employees' concerns about the DoD OIG's internal processes to protect whistleblowers in complaints involving other DoD OIG employees and leaders. The GAO's presentation of the data may leave a misleading impression, because of the focus on the small number of respondents who had negative impressions of the internal processes. In fact, the survey results show that more than 80 percent of respondents either believed that the DoD OIG's internal processes protected whistleblower confidentiality somewhat or very well, or did not know whether they did so. Only 14 percent of respondents expressed a belief that internal processes did not protect confidentiality or did so only slightly.

We also believe the portions of the report addressing restrictions on DoD OIG employee access to sensitive whistleblower information needs further context. The report referred to a lack of cross-directorate access controls within the DoD OIG's Administrative Investigations (AI) Directorate – including the DoD Hotline, the Investigations of Senior Officials unit, and Whistleblower Reprisal Investigations unit. However, it is important to note that while some records, for a period of time, may have been accessible to DoD OIG employees within those AI units who were not working on the particular matter, and the DoD Office of General Counsel and Office of Professional Responsibility, there is no evidence that any person without a need to know actually accessed any records containing sensitive whistleblower information. To be clear, no one outside the DoD OIG – or even outside AI, the DoD Office of General Counsel, or the DoD OIG Office of Professional Responsibility – had access to any of those records.

Further, it is important to note that all the instances of potential accessibility noted by GAO were first identified by DoD OIG employees, and that when the DoD OIG became aware of such issues it took corrective action to resolve the potential access issue. In one instance, for example, an error in the management of system permissions for SharePoint, which created an accessibility issue, was resolved approximately 48 hours after an AI leader first brought the error to systems administrators' attention. When system administrators corrected the error, they also locked all users out of the SharePoint to avoid unintentional access within the OIG to any protected records.

Most important, as noted above, there is no evidence that anyone without a need to know ever accessed any of these records. The GAO's report – and particularly the report's Highlights – do not make this point as clearly as it could.

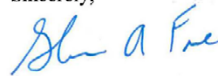
**Appendix V: Comments from the Department
of Defense**

DoD OIG Response to GAO Recommendations

Finally, as noted above, we concur with the GAO's recommendations and will seek to implement them in a timely manner. We believe they will help us to continue our substantial improvements to the whistleblower protection program and our handling of whistleblower complaints.

If you have any questions, please contact me or David A. Core, Associate General Counsel.

Sincerely,



Glenn A. Fine
Principal Deputy Inspector General
Performing the Duties of Inspector General

Enclosures
As stated

Cc:
The Inspector General, U.S. Army
The Naval Inspector General
The Air Force Inspector General
The Inspector General, Marine Corps



DEPARTMENT OF THE ARMY
OFFICE OF THE INSPECTOR GENERAL
1700 ARMY PENTAGON
WASHINGTON, DC 20310-1700

SAIG-AC

14 January 2019

MEMORANDUM FOR Department of Defense Office of Inspector General, ATTN:
David A. Core, Associate General Counsel, 4800 Mark Center Drive, Alexandria, VA
22350-1500

SUBJECT: U.S. Army Inspector General Response to the Government Accountability
Office Draft Report, "Whistleblower Protection", dated January 2019

1. We reviewed the draft report and concur with the findings presented. However, we would like to provide additional background regarding two areas of interest.

2. The Government Accountability Office (GAO) noted timeliness of complaint resolution is a challenge across the Department of Defense. We agree. Over the last five years, the United States Army Inspector General Agency (USAIGA) invested significant resources to achieve improvements in case throughput and timeliness of case resolution. We reduced the whistleblower reprisal (WBR) case load by over 40% from 472 non-senior WBR cases in August 2016 to 278 cases as of 10 January 2019. While the draft report noted some actions to address timeliness of complaint notifications to the Department of Defense Inspector General (DoDIG), we are also working on several additional initiatives to include education, training, doctrinal refinements, escalation strategies, and increased leader emphasis. Additionally, we collaboratively made specific recommendations pending implementation in the DoDIG led High Level Working Group.

3. The second area of interest concerns access to IG records within the Army Inspector General database of record, IGARS. While the draft report indicates individuals could have access to sensitive information pertaining to cases where they may not have a need-to-know or involving complaints pertaining to inspectors general (IGs), the report did not identify the existing policy and procedural safeguards in place within the Army to minimize inappropriate access to such information. For example, most IGs are only granted access to IGARS after being centrally trained and credentialed. Moreover, access is only granted through an IG leader driven process ultimately approved at the USAIGA level. Our policies and procedures achieve the appropriate balance between limiting access and enhancing case processing efficiency. Most unit level IG offices are not robustly manned; most have less than ten personnel and some are as small as two personnel. Because each IG team member may be required to assist with any case within an office, we authorize IGs access to cases within their office. At higher levels, such as this headquarters level, IGs have greater access but only in accordance with established guidelines, appropriate authorization,

SAIG-AC

SUBJECT: U.S. Army Inspector General Response to the Government Accountability
Office Draft Report, "Whistleblower Protection", dated January 2019

and that which is necessary to perform assigned duties. In the event of an allegation against an IG, the IG's Directing Authority (Commander) and several USAIGA senior leaders, to include The Inspector General, are involved in the decision making process that reviews the circumstances and decides whether to suspend or remove that individual's access to IG records. While it is possible that an IG could inappropriately access information, the processes in place provide judicious access and control necessary to achieve an appropriate balance between efficient operations and minimizing risk.

4. We concur with the major findings of the draft report, and appreciate this opportunity to provide additional comments for consideration. If you have questions pertaining to this correspondence, please contact our action officers, COL Karen Wrancher, (703) 545-4201 or Mr. Robert Nelson, (703) 545-1858.


LESLIE C. SMITH
Lieutenant General, USA
The Inspector General



Office of the Secretary

DEPARTMENT OF THE AIR FORCE
WASHINGTON DC

January 23, 2019

MEMORANDUM FOR DEPARTMENT OF DEFENSE INSPECTOR GENERAL

FROM: SAF/IG

SUBJECT: GAO Draft Report, GAO-19-198

Attached is our response to the GAO Draft Report GAO-19-198, 'WHISTLEBLOWER PROTECTION: Analysis of DoD's Actions to Improved Case Timeliness and Safeguard Confidentiality,' dated December 21, 2019 (GAO Code 101192)."

A handwritten signature in black ink, appearing to read "SAMI D. SAID", is positioned above the typed name and title.

SAMI D. SAID
Major General, USAF
Deputy Inspector General

Attachment
AF Response to Recommendations (101192)

GAO DRAFT REPORT DATED DECEMBER 19, 2018
GAO-19-198 (GAO CODE 101192)

“WHISTLEBLOWER PROTECTION: ANALYSIS OF DOD’S ACTIONS TO IMPROVE
CASE TIMELINESS AND SAFEGUARD CONFIDENTIALITY”

DEPARTMENT OF DEFENSE COMMENTS
TO THE GAO RECOMMENDATION

RECOMMENDATION: The Air Force Inspector General should establish procedures to fully reflect and implement DOD policy on the protection of whistleblower confidentiality.

DoD RESPONSE: Air Force Instruction (AFI) 90-301, *Inspector General Complaints Resolution*, 28 Dec 18, Chapter 3 paragraph 3.2.1. states that “At the time the IG receives a complaint, he or she will advise the complainant:

3.2.1.1.2 The Inspector General shall not, after receipt of a complaint or information from an employee, disclose the identity of the employee without the consent of the employee, unless the Inspector General determines such disclosure is unavoidable during the course of the investigation and/or complaint analysis. (T-0).

The language is essentially the same as 5 United States Code Appendix § 7. The “T-0” indicates that no official in the Air Force, at any level, can waive the requirement to inform the complainant of the non-disclosure requirement.

RECOMMENDATION: The Air Force Inspector General should consider interim actions as the whistleblower enterprise case management system is being developed to help ensure that access for users of existing applications is limited to information that is necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

DoD RESPONSE: As noted in the recommendation, the Air Force plans to transition from its case management system to an enterprise case management system being developed by the DoD IG, and therefore no longer funds development its system. Nevertheless, the Air Force IG is exploring the ability of the Air Force Administrative Assistant, Enterprise Business Solutions (the office that maintains the Air Force case management system) to modify the system to more fully limit user access to data.

Appendix V: Comments from the Department
of Defense



DEPARTMENT OF THE NAVY
HEADQUARTERS, UNITED STATES MARINE CORPS
3000 MARINE CORPS PENTAGON
WASHINGTON, DC 20350-3000

IN REPLY REFER TO:
7510
DMCS-A
15 Jan 19

From: Head, Audit Coordination, Office of the Director,
Marine Corps Staff
To: Primary Action Officer, Office of the Inspector General,
U.S. Department of Defense

Subj: GAO DRAFT REPORT GAO-19-198, "WHISTLEBLOWER PROTECTION:
ANALYSIS OF DOD'S ACTIONS TO IMPROVE CASE TIMELINESS AND
SAFEGUARD CONFIDENTIALITY," DATED DECEMBER 21, 2018 (GAO
CODE 101192)

Ref: (a) DoDI 7650.02 w/Ch 1, GAO Reviews and Reports
(b) DoD WHS-ESD (GAO Affairs) Memo to DODIG dtd 2 JAN 19

Encl: (1) U.S. Marine Corps Responses

1. Reference (a) requires timely responses to GAO reviews and reports. Reference (b) provided guidance on responding to draft report GAO-19-198.

2. Enclosure (1) provides our comments to the subject draft report for OSD Primary Action Office consideration in its response to GAO.

3. I am your primary Marine Corps contact for enclosure (1), and can be reached at 703-693-9724/571-289-7082/or charles.dove@usmc.mil.


CHARLES K. DOVE

Copy to:
NAVINGEN (N14)
IGMC
CL
DC, P&R (MCMICP)

UNCLASSIFIED

**GAO DRAFT REPORT DATED 21 DECEMBER 2018
GAO-19-198 (101192)**

**“WHISTLEBLOWER PROTECTION: ANALYSIS OF DOD’S ACTIONS TO
IMPROVE CASE TIMELINESS AND SAFEGUARD CONFIDENTIALITY”**

**U.S. MARINE CORPS COMMENTS
TO GAO RECOMMENDATIONS**

GAO is making a total of 12 recommendations to the Department of Defense (DOD).
The 2 recommendations directed to the Marine Corps are:

RECOMMENDATION 4: The Marine Corps Inspector General should establish
procedures to fully reflect and implement DOD policy on the protection of whistleblower
confidentiality.

USMC RESPONSE: Inspector General of the Marine Corps (IGMC) concurs. DoD
OIG’s policy concerning protection of Complainant confidentiality, found in DoD
Instruction (DoDI) 7050.01, “DoD Hotline Program,” and which applies to all Military
Departments, derives from the Inspector General (IG) Act of 1978, Section 7(b):

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

DoD OIG’s Office for Administrative Investigations (AI) manual for investigations, dated
29 March 2016, elaborates for cases of whistleblower reprisal:

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.

IGMC’s policy follows DoD OIG’s guidance. During the complaint intake process and
the initial clarification interview with a Complainant, IGMC personnel explain that
IGMC never can guarantee confidentiality and that whistleblower reprisal investigations
require disclosure of whistleblowers’ names in order to conduct the investigation. Unlike
other services, IGMC does not task military whistleblower reprisal investigations to
personnel in other offices or organizations. Only IGMC investigators conduct military
whistleblower reprisal investigations within the Marine Corps (for the rare circumstance

UNCLASSIFIED

1

Encl (1)

UNCLASSIFIED

when IGMC is conflicted and cannot conduct a certain investigation, a service level Naval IG or DoD OIG investigator do so on IGMC's behalf).

Marine Corps Order (MCO) 5370.8A, "Marine Corps Hotline Program," which is currently under revision, requires IGMC and its lower echelon Command Inspectors General (CIG) to comply with DoDI 7050.01 and DoD Directive (DoDD) 7060.01, "Military Whistleblower Reprisal." IGMC's own written guidance does not specifically address the requirement to protect Complainant confidentiality because DoD publications, which require compliance from all Marine Corps IGs, already articulate the requirement.

IGMC concurs with GAO that technical flaws in IGMC's Case Management System (CMS), which sometimes cause IGMC's protection of whistleblower confidentiality to fail, should never occur, that IGMC must correct the problem, and that IGMC's solution must reflect DoD OIG policy. IGMC will soon be able to implement reliable procedures to restrict access to whistleblower information when IGMC's new database, Case Action Manager (CAM), which is currently in production, becomes active. IGMC previously identified the flaw GAO references in recommendation 11, and included strict information access controls in CAM's functions. IGMC estimates transitioning to CAM during September 2019.

To improve IGMC's compliance with all investigative standards, in December 2018, IGMC hired a GS-15 Director of Investigations, with supervisory authority for all matters related to Marine Corps IG investigations.

RECOMMENDATION 11: The Marine Corps Inspector General should develop a plan to ensure that its redesigned whistleblower management application restricts user access information based on what is needed to accomplish assigned tasks in accordance with organizational missions and business functions.

USMC RESPONSE: IGMC concurs. IGMC's new, custom case management system, CAM, which is currently in production, will restrict user access information based on what is needed to accomplish assigned tasks in accordance with organizational missions and business functions. IGMC estimates transitioning to CAM during September 2019.



C. E. SHELTON
Deputy
Inspector General of the Marine Corps

UNCLASSIFIED

2

Encl (1)

Appendix VI: GAO Contact and Staff Acknowledgments

GAO Contact

Brenda S. Farrell, (202) 512-3604 or farrellb@gao.gov

Staff Acknowledgments

In addition to the contact named above, Alissa Czyz (Assistant Director), Tracy Barnes, Amy Bush, Nicole Collier, Ryan D'Amore, Chad Hinsch, Linda Keefer, Kevin Keith, Amie Lesser, Serena Lo, Michael Silver, and Lillian Yob made key contributions to this report.

Related GAO Products

Office of Special Counsel: Actions Needed to Improve Processing of Prohibited Personnel Practice and Whistleblower Disclosure Cases. [GAO-18-400](#). Washington, D.C.: June 14, 2018.

NASA Contractor Whistleblowers: Steps Taken to Implement Program but Improvements to Timeliness and Guidance Needed. [GAO-18-262](#). Washington, D.C.: March 8, 2018.

Whistleblower Protection: Opportunities Exist for DOD to Improve the Timeliness and Quality of Civilian and Contractor Reprisal Investigations. [GAO-17-506](#). Washington, D.C.: September 29, 2017.

Contractor Whistleblower Protections Pilot Program: Improvements Needed to Ensure Effective Implementation. [GAO-17-227](#). Washington, D.C.: March 2, 2017.

Whistleblower Protection: Additional Actions Would Improve Recording and Reporting of Appeals Data. [GAO-17-110](#). Washington, D.C.: November 28, 2016.

Whistleblower Protection: DOD Has Improved Oversight for Reprisal Investigations but Can Take Additional Actions to Standardize Process and Reporting. [GAO-16-860T](#). Washington, D.C.: September 7, 2016.

Department of Energy: Whistleblower Protections Need Strengthening. [GAO-16-618](#). Washington, D.C.: July 11, 2016.

Whistleblower Protection: DOD Needs to Enhance Oversight of Military Whistleblower Reprisal Investigations. [GAO-15-477](#). Washington, D.C.: May 7, 2015.

Whistleblower Protection: Additional Actions Needed to Improve DOJ's Handling of FBI Retaliation Complaints. [GAO-15-112](#). Washington, D.C.: January 23, 2015.

Whistleblower Protection Program: Opportunities Exist for OSHA and DOT to Strengthen Collaborative Mechanisms. [GAO-14-286](#). Washington, D.C.: March 19, 2014.

Whistleblower Protection: Actions Needed to Improve DOD's Military Whistleblower Reprisal Program. [GAO-12-362](#). Washington, D.C.: February 22, 2012.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (<https://www.gao.gov>). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to <https://www.gao.gov> and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, <https://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on [Facebook](#), [Flickr](#), [Twitter](#), and [YouTube](#).
Subscribe to our [RSS Feeds](#) or [E-mail Updates](#). Listen to our [Podcasts](#).
Visit GAO on the web at <https://www.gao.gov>.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: <https://www.gao.gov/fraudnet/fraudnet.htm>

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

Orice Williams Brown, Managing Director, WilliamsO@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800 U.S. Government Accountability Office, 441 G Street NW, Room 7149 Washington, DC 20548

Strategic Planning and External Liaison

James-Christian Blockwood, Managing Director, spel@gao.gov, (202) 512-4707 U.S. Government Accountability Office, 441 G Street NW, Room 7814, Washington, DC 20548

