United States Government Accountability Office

Report to Congressional Requesters

September 2020

WHISTLEBLOWER PROTECTION

Actions Needed to Strengthen Selected Intelligence Community Offices of Inspector General Programs

GAO-20-699

September 2020

WHISTLEBLOWER PROTECTION

Actions Needed to Strengthen Selected Intelligence Community Offices of Inspector General Programs

GAO Highlights

Highlights of GAO-20-699, a report to congressional requesters

Why GAO Did This Study

Whistleblowers play an important role in safeguarding the federal government against waste, fraud, and abuse. The OIGs across the government oversee investigations of whistleblower complaints, which can include protecting whistleblowers from reprisal. Whistleblowers in the IC face unique challenges due to the sensitive and classified nature of their work.

GAO was asked to review whistleblower protection programs managed by selected IC-element OIGs. This report examines (1) the number and time frames of investigations into complaints that selected IC-element OIGs received in fiscal years 2017 and 2018, and the extent to which selected IC-element OIGs have established timeliness objectives for these investigations; (2) the extent to which selected IC-element OIGs have implemented quality standards and processes for their investigation programs; (3) the extent to which selected IC-element OIGs have established training requirements for investigators; and (4) the extent to which selected IC-element OIGs have met notification and reporting requirements for investigative activities. This is a public version of a sensitive report that GAO issued in June 2020. Information that the IC elements deemed sensitive has been omitted.

GAO selected the ICIG and the OIGs of five of the largest IC elements for review. GAO analyzed time frames for all closed investigations of complaints received in fiscal years 2017 and 2018; reviewed OIG policies, procedures, training requirements, and semiannual reports to Congress; conducted interviews with 39 OIG

What GAO Found

The six Intelligence Community (IC)-element Offices of Inspectors General (OIG) that GAO reviewed collectively received 5,794 complaints from October 1, 2016, through September 30, 2018, and opened 960 investigations based on those complaints. Of the 960 investigations, IC-element OIGs had closed 873 (about 91 percent) as of August 2019, with an average case time ranging from 113 to 410 days to complete. Eighty-seven cases remained open as of August 2019, with the average open case time being 589 days. The number of investigations at each IC-element OIG varied widely based on factors such as the number of complaints received and each OIG's determination on when to convert a complaint into an investigation. An OIG may decide not to convert a complaint into an investigation if the complaint lacks credibility or sufficient detail, or may refer the complainant to IC-element management or to another OIG if the complaint involves matters that are outside the OIG's authority to investigate.

Four of the IC-element OIGs—the Central Intelligence Agency (CIA) OIG, the Defense Intelligence Agency (DIA) OIG, the National Reconnaissance Office (NRO) OIG, and the National Security Agency (NSA) OIG—have a 180-days or fewer timeliness objective for their investigations. The procedures for the remaining two OIGs—the Inspector General of the Intelligence Community (ICIG) and the National Geospatial-Intelligence Agency (NGA) OIG—state that investigations should be conducted and reported in a timely manner. Other than those prescribed by statute, the ICIG and NGA OIG have not established timeliness objectives for their investigations. Establishing timeliness objectives could improve the OIGs' ability to efficiently manage investigation time frames and to inform potential whistleblowers of these time frames.

All of the selected IC-element OIG investigations units have implemented some quality assurance standards and processes, such as including codes of conduct and ethical and professional standards in their guidance. However, the extent to which they have implemented processes to maintain guidance, conduct routine quality assurance reviews, and plan investigations varies (see table).

Implementation of Quality Assurance Standards and Practices by Selected IC-element OIG Investigations Units

	ICIG	CIA OIG	DIA OIG	NGA OIG	NRO OIG	NSA OIG
Regular updates of investigation guidance or procedures	—	—	—	✓	—	✓
Internal quality assurance review routinely conducted	—	—	✓	—	—	—
External quality assurance review routinely conducted	—	✓	—	—	—	—
Required use of documented investigative plans	✓	✓	✓	✓	—	✓

Legend: ✓ = standard or practice implemented; — = standard or practice not implemented.

Source: GAO analysis of IC-element OIG investigative policies and procedures. | GAO-20-699

investigators; and reviewed a selection of case files for senior leaders and reprisal cases from October 1, 2016, through March 31, 2018.

What GAO Recommends

GAO is making 23 recommendations, including that selected IC-element OIGs establish timeliness objectives for investigations, implement or enhance quality assurance programs, establish training plans, and take steps to ensure that notifications to complainants in reprisal cases occur. The selected IC-element OIGs concurred with the recommendations and discussed steps they planned to take to implement them.

View GAO-20-699. For more information, contact Brenda S. Farrell at (202) 512-3604, farrellb@gao.gov or Brian M. Mazanec at (202) 512-5130, mazanecb@gao.gov.

- The Council of Inspectors General on Integrity and Efficiency's (CIGIE) *Quality Standards for Investigations* states that organizations should facilitate due professional care by establishing written investigative policies and procedures via handbooks, manuals, or similar mechanisms that are revised regularly according to evolving laws, regulations, and executive orders. By establishing processes to regularly update their procedures, the ICIG, CIA OIG, DIA OIG, and NRO OIG could better ensure that their policies and procedures will remain consistent with evolving laws, regulations, Executive Orders, and CIGIE standards.
- Additionally, CIGIE's *Quality Standards for Federal Offices of Inspector General* requires OIGs to establish and maintain a quality assurance program.
- The standards further state that internal and external quality assurance reviews are the two components of an OIG's quality assurance program, which is an evaluative effort conducted by reviewers independent of the unit being reviewed to ensure that the overall work of the OIG meets appropriate standards. Developing quality assurance programs that incorporate both types of reviews, as appropriate, could help ensure that the IC-element OIGs adhere to OIG procedures and prescribed standards, regulations, and legislation, as well as identify any areas in need of improvement.
- Further, CIGIE *Quality Standards for Investigations* states that case-specific priorities must be established and objectives developed to ensure that tasks are performed efficiently and effectively. CIGIE's standards state that this may best be achieved, in part, by preparing case-specific plans and strategies. Establishing a requirement that investigators use documented investigative plans for all investigations could facilitate NRO OIG management's oversight of investigations and help ensure that investigative steps are prioritized and performed efficiently and effectively.

CIA OIG, DIA OIG, and NGA OIG have training plans or approaches that are consistent with CIGIE's quality standards for investigator training. However, while ICIG, NRO OIG, and NSA OIG have basic training requirements and tools to manage training, those OIGs have not established training requirements for their investigators that are linked to the requisite knowledge, skills, and abilities, appropriate to their career progression, and part of a documented training plan. Doing so would help the ICIG, NRO OIG, and NSA OIG ensure that their investigators collectively possess a consistent set of professional proficiencies aligned with CIGIE's quality standards throughout their entire career progression.

Most of the IC-element OIGs GAO reviewed consistently met congressional reporting requirements for the investigations and semiannual reports GAO reviewed. The ICIG did not fully meet one reporting requirement in seven of the eight semiannual reports that GAO reviewed. However, its most recent report, which covers April through September 2019, met this reporting requirement by including statistics on the total number and type of investigations it conducted. Further, three of the six selected IC-element OIGs—the DIA, NGA, and NRO OIGs—did not consistently document notifications to complainants in the reprisal investigation case files GAO reviewed. Taking steps to ensure that notifications to complainants in such cases occur and are documented in the case files would provide these OIGs with greater assurance that they consistently inform complainants of the status of their investigations and their rights as whistleblowers.

Contents

Letter		1
	Background	6
	Selected OIGs Closed 873 Investigations of Complaints Received in Fiscal Years 2017 and 2018, and Two of Six IC-Element OIGs Do Not Have Timeliness Objectives	16
	Each IC-Element OIG Has Implemented Some Quality Assurance Processes, but Some OIGs Do Not Regularly Update Guidance or Conduct Routine Quality Assurance Reviews	21
	Investigators Attend a Variety of Training Courses, but Three of Six IC-Element OIGs Have Not Established Training Requirements in a Documented Plan	31
	Most Selected IC-Element OIGs Consistently Met Congressional Notification and Reporting Requirements, but Not All of Them Always Documented Notifications to Complainants	36
	Conclusions	47
	Recommendations for Executive Action	47
	Agency Comments and Our Evaluation	50
Appendix I	Intelligence Community (IC)-Element Offices of Inspector General's (OIG) Hotline and Investigative Processes	51
Appendix II	Statistics for Selected Intelligence Community (IC)-Element Offices of Inspector General (OIG) Investigations	56
Appendix III	List of Intelligence Community (IC) Whistleblower Protection Laws, Policies, and Quality Standards	63
Appendix IV	Comments from the Inspector General of the Intelligence Community	66
Appendix V	Comments from the Inspector General of the Central Intelligence Agency	70

Appendix VI	Comments from the Inspector General of the Defense Intelligence Agency	72
Appendix VII	Comments from the Inspector General of the National Geospatial-Intelligence Agency	75
Appendix VIII	Comments from the Inspector General of the National Reconnaissance Office	77
Appendix IX	Comments from the Inspector General of the National Security Agency	80
Appendix X	Comments from the Department of Defense	83
Appendix XI	GAO Contacts and Staff Acknowledgments	84

Tables

Table 1: List of 17 Intelligence Community (IC) Elements 7
Table 2: Defense Intelligence Community Office of Inspector General (OIG) Compliance with Selected Statutory Requirements for Semiannual Reports, Fiscal Years 2017 and 2018 38
Table 3: Intelligence Community Inspector General and Central Intelligence Agency Inspector General Compliance with Selected Statutory Requirements for Semiannual Reports 39
Table 4: Selected Intelligence Community (IC)-Element Policies and Office of Inspector General (OIG) Procedures for Communications to Whistleblowers in Reprisal Investigations 45

Table 5: Selected Intelligence Community (IC)-Element Office of Inspector General (OIG) Procedures for Documenting Whistleblower Communications 46

Figures

Figure 1: Whistleblower Protections for Intelligence Community (IC) Employees and Contractors and Military Servicemembers 9
Figure 2: Time Frame Statistics for Investigations of Complaints Received in Fiscal Years 2017 and 2018, as of August 2019 18
Figure 3: Inspector General of the Intelligence Community (ICIG) Hotline and Investigative Process 52
Figure 4: Central Intelligence Agency (CIA) Office of Inspector General (OIG) Hotline and Investigative Process 53
Figure 5: Defense Intelligence Agency (DIA) Office of Inspector General (OIG) Hotline and Investigative Process 53
Figure 6: National Geospatial-Intelligence Agency (NGA) Office of Inspector General (OIG) Hotline and Investigative Process 54
Figure 7: National Reconnaissance Office (NRO) Office of Inspector General (OIG) Hotline and Investigative Process 54
Figure 8: National Security Agency (NSA) Office of Inspector General (OIG) Hotline and Investigative Process 55
Figure 9: Complaints Received and Investigated by Intelligence Community (IC)-element Offices of Inspector General (OIG) in Fiscal Years 2017 and 2018 56
Figure 10: Inspector General of the Intelligence Community (ICIG) Time Frames for Closed Investigations of Complaints Received in Fiscal Years 2017 and 2018 57
Figure 11: Central Intelligence Agency (CIA) Office of Inspector General (OIG) Time Frames for Closed Investigations of Complaints Received in Fiscal Years 2017 and 2018 58
Figure 12: Defense Intelligence Agency (DIA) Office of Inspector General (OIG) Time Frames for Closed Investigations of Complaints Received in Fiscal Years 2017 and 2018 59
Figure 13: National Geospatial-Intelligence Agency (NGA) Office of Inspector General (OIG) Time Frames for Closed Investigations of Complaints Received in Fiscal Years 2017 and 2018 60

Figure 14: National Reconnaissance Office (NRO) Office of Inspector General (OIG) Time Frames for Closed Investigations of Complaints Received in Fiscal Years 2017 and 2018 61
Figure 15: National Security Agency (NSA) Office of Inspector General (OIG) Time Frames for Closed Investigations of Complaints Received in Fiscal Years 2017 and 2018 62

Abbreviations

CIA	Central Intelligence Agency
CIGIE	Council of Inspectors General for Integrity and Efficiency
DIA	Defense Intelligence Agency
DOD	Department of Defense
IC	Intelligence Community
ICIG	Inspector General of the Intelligence Community
NGA	National Geospatial-Intelligence Agency
NRO	National Reconnaissance Office
NSA	National Security Agency
OIG	Office of Inspector General

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.

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

September 25, 2020

The Honorable Mark R. Warner
Vice Chairman
Select Committee on Intelligence
United Stated Senate

The Honorable Susan M. Collins
United States Senate

The Honorable Charles E. Grassley
United States Senate

The Honorable Ron Wyden
United States Senate

Whistleblowers play an important role in safeguarding the federal government against waste, fraud, and abuse, and their willingness to come forward can contribute to improvements in government operations.[1] The Offices of Inspector General (OIG) are responsible for overseeing the investigation of complaints alleging waste, fraud, and abuse in their respective agencies in a timely and fair manner. This includes the protection of whistleblowers from prohibited personnel practices, including reprisal. Whistleblowers in the Intelligence Community (IC) present unique challenges for OIGs, due in part to the need to protect classified information that is likely to be involved in an IC-related incident or complaint. Members of Congress have raised questions about the timeliness and integrity of investigations conducted by IC-element OIGs and whether their responsibilities are being uniformly fulfilled.

We reported in 2017 that the Department of Defense (DOD) OIG had conducted oversight of investigations involving defense civilian intelligence personnel conducted by some of the defense IC-element OIGs. However, the DOD OIG and the defense IC-element OIGs—the Defense Intelligence Agency (DIA) OIG, the National Geospatial-Intelligence Agency (NGA) OIG, the National Reconnaissance Office (NRO) OIG, and the National Security Agency (NSA) OIG—had not fully

[1]In this report, we use the term “whistleblower” to refer to any federal employee, military servicemember, contractor, or grantee who lawfully discloses suspected wrongdoing to an authorized recipient, regardless of his or her reprisal status or the nature of his or her disclosure.

addressed all oversight requirements. We recommended that the DOD OIG work in coordination with the Secretary of Defense, the Under Secretary of Defense for Intelligence, and the defense IC-element OIGs to establish a process to fully implement oversight requirements so that the DOD OIG (1) receives notifications of all allegations received by the defense IC-element OIGs, (2) reviews all defense IC-element OIG determinations not to investigate allegations, and (3) reviews all investigations conducted by the defense IC-element OIGs to ensure that the proper standards of proof were applied in the investigations, among other things.[2] The DOD OIG concurred with this recommendation. In July 2019, the DOD OIG implemented the recommendation by signing a memorandum of understanding with the defense intelligence OIGs to clarify aspects of the relationship between the defense intelligence OIGs and the DOD OIG. We discuss these actions in more detail later in this report.

You asked us to review the whistleblower protection programs that the IC-element OIGs manage. This report examines (1) the number and time frames of investigations into complaints that selected IC-element OIGs received in fiscal years 2017 and 2018, and the extent to which IC-element OIGs have timeliness objectives for these investigations; (2) the extent to which selected IC-element OIGs have implemented quality standards and processes for their investigation programs; (3) the extent to which selected IC-element OIGs have established training requirements for investigators; and (4) the extent to which selected IC-element OIGs have met notification and reporting requirements for investigative activities, and actions they are taking to address any associated challenges.

This report is a public version of a sensitive report that we issued in June 2020.[3] The IC elements deemed some of the information in our June report to be sensitive, which must be protected from public disclosure. Therefore, this report omits sensitive information about whistleblower investigation statistics for some of the IC elements included in our review. Although the information provided in this report is more limited, the report

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

[3]GAO, *Whistleblower Protection: Actions Needed to Strengthen Selected Intelligence Community Offices of Inspector General Programs,* GAO-20-201SU (Washington, D.C.: June 19, 2020).

addresses the same objectives as the sensitive report and uses the same methodology.

For all of our objectives, we selected six IC-element OIGs—the Inspector General of the Intelligence Community (ICIG), the Central Intelligence Agency (CIA) OIG, the DIA OIG, the NSA OIG, the NGA OIG, and the NRO OIG—to review. We selected ICIG and these five elements because they represent the largest of the 17 IC elements that we have not previously reviewed.[4] Moreover, for objectives 2-4 we focused on two types of cases: whistleblower reprisal cases and cases involving allegations against senior leaders.[5] We selected these types of cases because IC-element policies state that these can be some of the most sensitive and high-profile cases.

For our first objective, we obtained case management data from the six IC-element OIGs for complaints received from October 1, 2016, through September 30, 2018. We focused on this time frame because it constituted the most complete and recent data available in all six of the IC-element OIGs' case-management systems at the time of our review and allowed IC-element OIGs a reasonable period of time (that is, about

[4]We did not include one of the largest IC elements—the Federal Bureau of Investigation (FBI)—in this review, because we previously reviewed the Department of Justice (DOJ) OIG's efforts to protect whistleblowers employed by the FBI, in 2015, and we are continuing to monitor DOJ's efforts to implement our recommendations. See GAO, *Whistleblower Protection: Additional Actions Needed to Improve DOJ's Handling of FBI Retaliation Complaints,* GAO-15-112 (Washington, D.C.: Jan. 23, 2015). We made eight recommendations in that report, including that the Attorney General clarify in all current, relevant DOJ guidance and communications, including FBI guidance and communications, to whom FBI employees may make protected disclosures. The Department of Justice agreed with all eight recommendations and has implemented two of them. As of November 2019, DOJ had not yet implemented the remaining six recommendations.

[5]Among other provisions, Part A of Presidential Policy Directive 19 prohibits any officer or employee of an IC element who has authority to take, direct others to take, recommend, or approve any personnel action from taking or failing to take, or threatening to take or fail to take, a personnel action with respect to any employee serving in an IC element as a reprisal for a protected disclosure. Part B of Presidential Policy Directive 19 prohibits any officer or employee of an IC element from taking or failing to take, or threating to take or fail to take, any action affecting an employee's eligibility for access to classified information as a reprisal for a protected disclosure. For the purposes of this report, senior leader investigations include any investigation into an allegation made against (1) a military officer of flag or general officer rank; (2) a civilian in the Senior Executive Service or Defense Intelligence Senior Executive Service; (3) a civilian intelligence official designated as a Defense Intelligence Senior Leader; or (4) an intelligence official in a politically appointed position.

11 months) to process complaints received near the end of the selected time frame. We used these data to calculate the time it took each IC-element OIG to complete closed investigations, from the date when each complaint was received to the date when the final report or closing document was signed. To determine how long ongoing investigations have been open, we calculated the number of days between the date when each complaint was received to the date when the data were provided to us or retrieved from the respective OIG's case management systems.[6] To assess the reliability of the case management data, we interviewed knowledgeable officials and examined the data for obvious errors. We determined that the data were sufficiently reliable for the purposes of identifying the number, type, and status of cases and examining their overall time frames.

We also reviewed policies and guidance of the selected IC-element OIGs for conducting investigations to determine whether these documents contained objectives or requirements related to time frames for completing investigations and specific investigative steps. We evaluated these timeliness objectives and requirements against relevant Council of the Inspectors General on Integrity and Efficiency (CIGIE) quality standards and standards for internal control. We also interviewed IC-element OIG officials and conducted semi-structured interviews with all 39 IC-element OIG investigators who had experience in conducting reprisal or senior leader investigations at the time of our review. We obtained their perspectives on the time frames required to complete investigations and any challenges that might affect the investigators' ability to meet timeliness objectives.

For our second objective, we reviewed policies and guidance of the selected IC-element OIGs for conducting investigations and analyzed these documents against relevant CIGIE quality standards. To determine the extent to which the selected IC-element OIGs followed and documented key quality assurance processes, we reviewed case files for 28 whistleblower reprisal and senior leader cases—including both substantiated and unsubstantiated cases—closed by the selected IC-element OIGs from October 1, 2016, through March 31, 2018, including all seven such cases closed by the CIA OIG and all four cases closed by the NRO OIG. We randomly selected five out of the seven cases closed

[6]For each IC-element OIG, the case status—that is, open or closed—and days open are current as of the following dates: ICIG (August 9, 2019); CIA OIG (August 6, 2019); DIA OIG (July 2, 2019); NGA OIG (July 1, 2019); NRO OIG (June 26, 2019); NSA OIG (June 28, 2019).

by the NSA OIG. Due to the number of cases that the NGA OIG and DIA OIG closed in this time frame, we randomly selected six out of 36 cases at the NGA OIG and six out of 38 cases at the DIA OIG. The ICIG did not close any whistleblower reprisal or senior leader investigations in this time frame. We focused on this time frame because it constituted the most complete and recent data available in all six of the IC-element OIGs' case-management systems at the time of our review. We also interviewed the 39 current IC-element investigators who had experience in conducting reprisal or senior leader investigations, to determine how they implement quality standards. We also reviewed the CIA OIG's quality assurance review reports and interviewed IC-element OIG officials to discuss any plans or challenges associated with conducting internal and external quality assurance reviews in the IC. We reviewed all information that related to key quality assurance processes against CIGIE quality standards and relevant standards for internal control.

For our third objective, we reviewed IC-element OIG policy and guidance documents for information on investigator training, including any required or suggested training. We compared the policy and guidance documents with CIGIE quality standards regarding training and *Standards for Internal Control in the Federal Government* related to demonstrating a commitment to competence and defining objectives and risk tolerances.[7] We also interviewed the 39 current IC-element OIG investigators who had experience in conducting reprisal or senior leader investigations to obtain their perspectives on required, suggested, and IC-specific training, and we discussed investigator training programs with IC-element OIG officials.

For our fourth objective, we reviewed applicable statutes, Presidential Policy Directive 19, and IC and DOD policies and procedures to identify the IC-element OIGs' notification and congressional reporting requirements related to reprisal and senior leader misconduct cases, urgent concerns, and semiannual reports. We reviewed semiannual reports to Congress covering fiscal years 2017 and 2018 from all six of the IC-element OIGs in our review.[8] We also reviewed semiannual reports for fiscal year 2019 from the ICIG because of additional

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

[8]We reviewed semiannual reports for the DIA, NGA, and NSA OIGs from October 1, 2016, through September 20, 2018. We reviewed NRO OIG semiannual reports from October 1, 2016 through March 31, 2018. We reviewed CIA OIG semiannual reports from October 1, 2014, through March 31, 2018, and ICIG semiannual reports from October 1, 2014, through September 30, 2019.

information ICIG officials told us they included in those reports. We compared these semiannual reports to applicable statutory requirements.

For the 28 selected case files discussed above, we reviewed documentation related to communications with complainants, as well as documentation of required congressional notifications. We also interviewed IC-element OIG officials to discuss any challenges with notification and reporting on whistleblower matters and any actions they are taking to address any challenges.

The performance audit upon which this report is based was conducted from January 2018 to June 2020 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. We subsequently worked with ICIG from June 2020 to August 2020 to prepare this public version of the original sensitive report for public release. This public version was also prepared in accordance with these standards.

Background

Mission and Organization of the IC and Inspectors General

The Director of National Intelligence serves as head of the IC and acts as the principal adviser to the President and National Security Council on intelligence matters related to national security. The IC is comprised of 17 executive branch agencies and organizations, generally referred to as IC elements. These IC elements include two independent agencies, eight elements within DOD, and seven elements across five other executive departments (see table 1).

Table 1: List of 17 Intelligence Community (IC) Elements

Independent elements	• Office of the Director of National Intelligence
	• Central Intelligence Agency
Elements within the Department of Defense	• Defense Intelligence Agency
	• National Security Agency
	• National Geospatial-Intelligence Agency
	• National Reconnaissance Office
	• U.S. Air Force Intelligence
	• U.S. Navy Intelligence
	• U.S. Army Intelligence
	• U.S. Marine Corps Intelligence
Elements in other departments	• Department of Energy's Office of Intelligence and Counterintelligence
	• Department of Homeland Security's Office of Intelligence and Analysis
	• Drug Enforcement Administration's Office of National Security Intelligence
	• Federal Bureau of Investigation's National Security Branch
	• Department of the Treasury's Office of Intelligence and Analysis
	• Department of State's Bureau of Intelligence and Research
	• U.S. Coast Guard Intelligence

Source: Office of the Director of National Intelligence data. | GAO-20-699

Note: Section 3003 of Title 50, United States Code, defines the IC as the elements listed in the table above as well as such other elements of any department or agency as designated by the President or jointly by the Director of National Intelligence and the head of the department or agency concerned, as an element of the IC.

The Inspector General Act of 1978, as amended, provides that the IGs of DIA, NGA, NRO, and NSA 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 safety.[9] Title 50 provides that the ICIG and CIA IG may receive and investigate complaints or information from any person concerning these matters.[10] Violation of the law may also include a violation of criminal law.

Whistleblower Protections for IC Personnel

Whistleblowers are protected from reprisal as a result of making a protected disclosure through various statutes, regulations, and presidential policy covering IC employees, military servicemembers, and contractors. Figure 1 summarizes the statutory and policy authorities

[9]See 5 U.S.C. App. § 7(a).

[10]See 50 U.S.C. § 3033(g) and 50 U.S.C. § 3517(e), respectively.

covering different categories of 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. Appendix III provides a list of additional policies and procedures that establish or implement whistleblower protections across the IC. A protected disclosure occurs when a whistleblower discloses information that the employee reasonably believes evidences (1) a violation of any federal law, rule, or regulation; or (2) mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety to an authorized recipient. 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.[11]

[11]See 50 U.S.C. § 3234.

Figure 1: Whistleblower Protections for Intelligence Community (IC) Employees and Contractors and Military Servicemembers

	IC employees, *including Defense Civilian Intelligence Personnel System employees and employees with eligibility or access to classified information*	**IC contractors, subcontractors, grantees, and subgrantees**	**Military servicemembers**
Authority	• Presidential Policy Directive 19 • 50 U.S.C. § 3234 • 5 U.S.C § 2302(b)(8) • 50 U.S.C. § 3341	• Presidential Policy Directive 19, Part B • 50 U.S.C. § 3234 • 50 U.S.C. § 3341	• 10 U.S.C. § 1034 • Presidential Policy Directive 19, Part B
Selected protected disclosures	A lawful disclosure of violation of law, rule, or regulation.		Violation of any law, rule, or regulation.
	Mismanagement.	Gross mismanagement.	
		Gross waste of funds.	
		Abuse of authority.	
	Substantial and specific danger to public health or safety.		
Selected prohibited personnel actions	Termination.		
	Reassignment.		
	Demotion.		
	Taking or withholding, or threatening to take or withhold, any action affecting an employee's eligibility for access to classified information.		
			Take (or threaten to take) an unfavorable personnel action, or withhold (or threaten to withhold) a favorable personnel action.
			The making of or threat to make any other significant change in duties or responsibilities not commensurate with the servicemember's grade.

Source: GAO analysis of statutes and Presidential Policy Directive 19. | GAO-20-699

Under the Intelligence Authorization Act for Fiscal Year 2014 and the Intelligence Authorization Act for Fiscal Year 2010, the DIA OIG, NGA OIG, NRO OIG, and NSA OIG have independent statutory authority to conduct investigations of reprisal complaints brought to them by employees in the Defense Civilian Intelligence Personnel System and military servicemembers.[12] The FISA Amendments Reauthorization Act of 2017 extended whistleblower reprisal protections to IC contractors, subcontractors, grantees, and subgrantees and designated the congressional intelligence committees, the Director of National Intelligence, ICIG, and the heads and IGs of IC elements as authorized recipients of protected disclosures.[13]

IC-element OIG Roles and Responsibilities for Investigating Whistleblower Complaints

IC-element OIGs are responsible for investigating allegations of misconduct or whistleblower reprisal and for operating hotline programs to receive and process allegations. IC employees and contractors, as well as military servicemembers and members of the general public, can report complaints or information concerning potential wrongdoing to a number of entities, including the directors, inspectors general, and other designated officials in their respective IC elements; the Director of National Intelligence; the Inspector General of the IC; and members and staff of the Senate Select Committee on Intelligence and House Permanent Select Committee on Intelligence. DOD contractors and civilian employees in the Defense Civilian Intelligence Personnel System may also make complaints to the Inspector General of DOD. The U.S. Office of Special Counsel and in most cases the Merit Systems Protection Board do not have the authority to receive, investigate, or review complaints from IC personnel.[14]

IC-element OIGs have processes for receiving, vetting, and investigating complaints. Each IC-element OIG operates a hotline program that is

[12]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) and codified at 5 U.S.C. Appendix §§ 8G and 12. The Defense Civilian Intelligence Personnel System is a pay-for-performance management system established in 2007 for DOD civilian employees of the defense intelligence community elements.

[13]Pub. L. No. 115-118, § 110, (2018).

[14]Certain civilian IC employees may appeal a prohibited personnel action to the Merit Systems Protection Board (MSPB). See, for example, *Gale M. Clarke vs. Department of Defense*, 2006 MSPB 211 (July 14, 2006), which held that an IC employee retains formerly held MSPB appeal rights when transferring from another agency or position if the agency fails to notify the employee that transfer to the IC agency relinquishes MSPB adverse action appeal rights.

responsible for receiving complaints; determining the credibility of the information initially provided by complainants; creating a record of the complaint in the OIG's case management system; and routing relevant information to the appropriate officials. Generally, upon receiving a complaint, hotline managers and supervisors may decide not to investigate the complaint if it lacks credibility or sufficient detail to conduct investigative work, or they may direct the complainant to IC-element management or to another OIG if the complaint involves matters that are outside the OIG's authority to investigate potential fraud, waste, or abuse and potential violations of law, regulation, or policy. Hotline officials may also refer certain complaints to another entity if (1) there is no possibility of disclosing the identity of the complainant or (2) the complainant consents to the referral when there is a possibility of disclosing his or her identity.

If hotline officials determine that a complaint is credible and within the purview of the OIG, they are typically to provide the complaint to the IC-element OIG's investigative managers and staff, who may further vet the complaint and determine whether to conduct a full investigation according to the respective OIG's processes and procedures. These processes and procedures may include a review by a committee of senior IC-element OIG officials, such as the Inspector General, the Deputy Inspector General, or the Assistant Inspector General for Investigations. Additionally, all six IC-element OIGs have procedures that include an initial fact-finding stage—which may be referred to as an inquiry, preliminary inquiry, or preliminary investigation, depending on the IC-element OIG—to determine whether a full investigation is needed to reach a conclusion on the substance of the complaint. Appendix I provides additional information and graphical depictions of each IC-element OIG's process for receiving, vetting, and investigating whistleblower complaints.

DOD OIG Oversight Role for Select Defense Intelligence OIG Cases

The DOD OIG is also responsible for conducting oversight of cases at the defense intelligence element OIGs (DIA OIG, NGA OIG, NRO OIG, and NSA OIG) that involve allegations of reprisal against whistleblowers in the Defense Civilian Intelligence Personnel System or misconduct by senior DOD officials. From 2013 through 2017, DOD Directive-Type Memorandum 13-008, which implemented Presidential Policy Directive 19 within DOD, required the defense intelligence element OIGs to notify the DOD OIG of whistleblower reprisal allegations they received from employees in the Defense Civilian Intelligence Personnel System. It also granted the DOD OIG the authority to retain such cases for investigation or refer them back to the component OIGs, in which case the DOD OIG

conducts oversight of the investigations. Directive-Type Memorandum 13-008 expired in January 2018.[15] In July 2019, the DOD OIG signed a memorandum of understanding with the defense intelligence OIGs to clarify aspects of the relationship between the defense intelligence OIGs and DOD OIG.

Current DOD policy requires that defense intelligence OIGs notify the DOD OIG when they receive an allegation involving senior DOD officials.[16] The DOD OIG may also receive complaints or information from employees of the defense intelligence elements and military servicemembers assigned to the IC. If a complainant chooses to make an allegation of any kind to the DOD OIG, the DOD OIG may elect to (1) dismiss the complaint if it is deemed frivolous, (2) investigate the complaint, or (3) refer the complaint to the appropriate IC-element OIG for disposition. According to DOD OIG officials, they elect to investigate all allegations of reprisal under Presidential Policy Directive 19, Part B, that involve DOD personnel.

ICIG Responsibilities for External Review Panels and the IC Inspectors General Forum

Within the IC, the ICIG has several additional authorities and responsibilities related to whistleblower protections. Specifically, Presidential Policy Directive 19, Part C, which was recently codified in the Damon Paul Nelson and Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020 states that IC employees who allege reprisal and exhaust the applicable review process may request an external review chaired by the ICIG, called an External Review Panel.[17] Under current ICIG guidance, employees who allege

[15]DOD, Directive-Type Memorandum 13-008, *DOD Implementation of Presidential Policy Directive 19*, (July 8, 2013, incorporating change 3, Feb. 9, 2016). An official with the Office of the Undersecretary of Defense for Intelligence—the organization that issued Directive-Type Memorandum 13-008—stated that DOD currently plans to incorporate Presidential Policy Directive 19 in a forthcoming revision to DOD Instruction 1400.25, Volume 2001, *DOD Civilian Personnel Management System: Defense Civilian Intelligence Personnel System (DCIPS) Introduction* (Dec. 29, 2008, incorporating change 1, Mar. 17, 2014).

[16]DOD Directive 5505.06, *Investigations of Allegations against Senior DOD Officials* (June 6, 2013).

[17]In the event that the employee alleging reprisal is an employee of the Office of the Director of National Intelligence and the ICIG conducted the initial review or finds other reason to recuse himself, ICIG policy states that the ICIG will be recused from the External Review Panel and another IG will serve as chair. This practice was recently codified in the Damon Paul Nelson and Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020, Pub. L. No. 116-92 (2019). See 50 U.S. Code § 3236(c)(2)(C)(ii).

reprisal have 45 days from receiving a written notification of the OIG's disposition of the allegation to request an External Review Panel from the ICIG, and the ICIG has an additional 45 days to decide, at his or her discretion, whether to convene an External Review Panel. If the ICIG decides to convene an External Review Panel, the ICIG then designates two other panel members from the Inspectors General of a selection of agencies identified in Section 3236 of Title 50, U.S. Code.[18]

In addition, section 3033 of Title 50, U.S. Code, gives the ICIG a coordination function among the various inspectors general within the IC and provides that the ICIG is to serve as chair of the IC Inspectors General Forum. The IC Inspectors General Forum consists of 12 IGs who have oversight responsibilities for IC elements and serves as a mechanism for informing its members of the work of individual members of the forum that may be of common interest and discussing questions about jurisdiction, among other matters. In its role as the chair of the IC Inspectors General Forum, the ICIG provides refresher training and updates on changes to whistleblower protection laws and regulations, among other things.

Employee Outreach and Awareness

Intelligence Community Directive 120, *Intelligence Community Whistleblower Protection* (Mar. 20, 2014) implements Presidential Policy Directive 19 for the IC, to include establishing policy to ensure that all personnel serving in the IC are aware of the protections and review processes available to individuals who make protected disclosures. Under Intelligence Community Directive 120, the heads of IC elements must ensure, through workforce communications upon entry on duty and annually thereafter, that their employees are aware of all applicable protections and review processes available to whistleblowers. The heads of IC elements are also to make this information easily and readily available to their employees.[19]

[18]The IGs identified in the Damon Paul Nelson and Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020 are the IGs of the Department of State, the Department of Treasury, the Department of Defense, the Department of Justice, the Department of Energy, the Department of Homeland Security, the Central Intelligence Agency, the Defense Intelligence Agency, the National Geospatial-Intelligence Agency, the National Reconnaissance Office, and the National Security Agency.

[19]Since the scope of this review focused solely on the activities of the IC-element OIGs, we did not evaluate the employee outreach and awareness activities of the heads of the IC elements.

Although Intelligence Community Directive 120 assigns responsibility for employee outreach and awareness to the heads of IC elements, all of the selected IC-element OIGs support their respective IC elements' workforce communications or provide training and awareness materials on whistleblower protections directly to IC employees. For example, each of the IC-element OIGs we reviewed maintain internal or external websites that provide information such as the IG's mission and statutory authorities, the options for submitting complaints to the OIG, and answers to frequently asked questions. Additionally, the ICIG, CIA OIG, DIA OIG, NGA OIG, and NRO OIG each produces pamphlets and fliers that provide information such as the protections available to whistleblowers, the required tests that an allegation must meet to constitute reprisal, the investigative process, and contact information for the OIG's hotline.

Furthermore, the NSA OIG provides briefings on whistleblower protections to NSA managers, contracting officers, and others, including new employees, and has developed whistleblower protection training materials and videos that have been incorporated into NSA's mandatory agency-wide training requirements. According to NSA OIG officials, the NSA Inspector General also created a Whistleblower Coordinator position, which is staffed by IG Counsel, and is available to all Agency employees and affiliates to address any questions regarding their rights and protections. ICIG reported that in 2018, it arranged for comment on the Office of the Director of National Intelligence's whistleblower protection training modules by NSA OIG. Additionally, the ICIG reported that it routinely distributes promotional materials that include the ICIG's logo and contact information.

The CIA OIG's Office of Investigations also maintains a separate outreach initiative aimed at educating CIA employees on whistleblower protections in the workplace. According to CIA OIG officials, all new CIA employees receive a briefing by senior CIA OIG staff explaining whistleblower protections and why such protections are important. The CIA OIG also briefs at senior CIA staff conferences where whistleblower retaliation program information is presented. During fraud awareness briefings to CIA employees and contractors, OIG investigators discuss whistleblower protections and the importance of whistleblowing.

Moreover, in 2018, the ICIG established a Center for Protected Disclosures to improve communication and outreach on whistleblower matters across the IC. The Center for Protected Disclosures was established to (1) receive and process whistleblower complaints through the ICIG's hotline program; (2) provide community outreach and guidance

to individuals seeking information about the options and protections afforded to whistleblowers in the IC; and (3) administer and review requests for External Review Panels. To support these activities, the ICIG reported creating additional positions in 2019, including a full-time Source Support Program Manager and a director for the Center for Protected Disclosures.[20]

CIGIE Standards

CIGIE's *Quality Standards for Federal Offices of Inspector General* and *Quality Standards for Investigations* establish professional standards to guide the management, operation, and conduct of OIGs and their staff.[21] Among other things, these standards state that OIG managers and staff are to adhere to ethical principles; maintain quality assurance for investigations; and exercise due professional care in conducting investigations. Collectively, CIGIE standards provide a set of overarching principles to which IGs should adhere in conducting their operations and provide a framework for conducting high-quality investigations.

CIGIE's *Quality Standards for Investigations* recognizes that members of the OIG community are widely diverse in their missions, authorities, staffing levels, funding, and day-to-day operations. As such, the *Quality Standards for Investigations* are designed to be comprehensive, relevant, and sufficiently broad to accommodate a full range of OIG criminal, civil, and administrative investigations across the CIGIE membership. These standards allow for each OIG that is a member of CIGIE to implement the quality standards in accordance with the OIG's particular mission, unique circumstances, and respective department or agency requirements. However, the *Quality Standards for Investigations* also states that certain foundational principles apply to any investigative organization.

The CIGIE Integrity Committee receives, reviews, and refers for investigation allegations of wrongdoing made against Inspectors General and designated staff members of an IG, among others.[22] Each Inspector General, including each of the IC-element OIGs, is required to submit a

[20]The ICIG's Source Support Program Manager provides guidance to whistleblowers and conducts outreach to the IC on whistleblower protections and training.

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

[22]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. App. § 11(d)(4)(B).

list of designated staff members to the CIGIE Integrity Committee Chairperson annually.

Selected OIGs Closed 873 Investigations of Complaints Received in Fiscal Years 2017 and 2018, and Two of Six IC-Element OIGs Do Not Have Timeliness Objectives

Selected IC-Element OIGs Closed about 91 Percent of Investigations of Complaints Received in Fiscal Years 2017 and 2018, but Time Frames Needed to Close the Investigations Varied

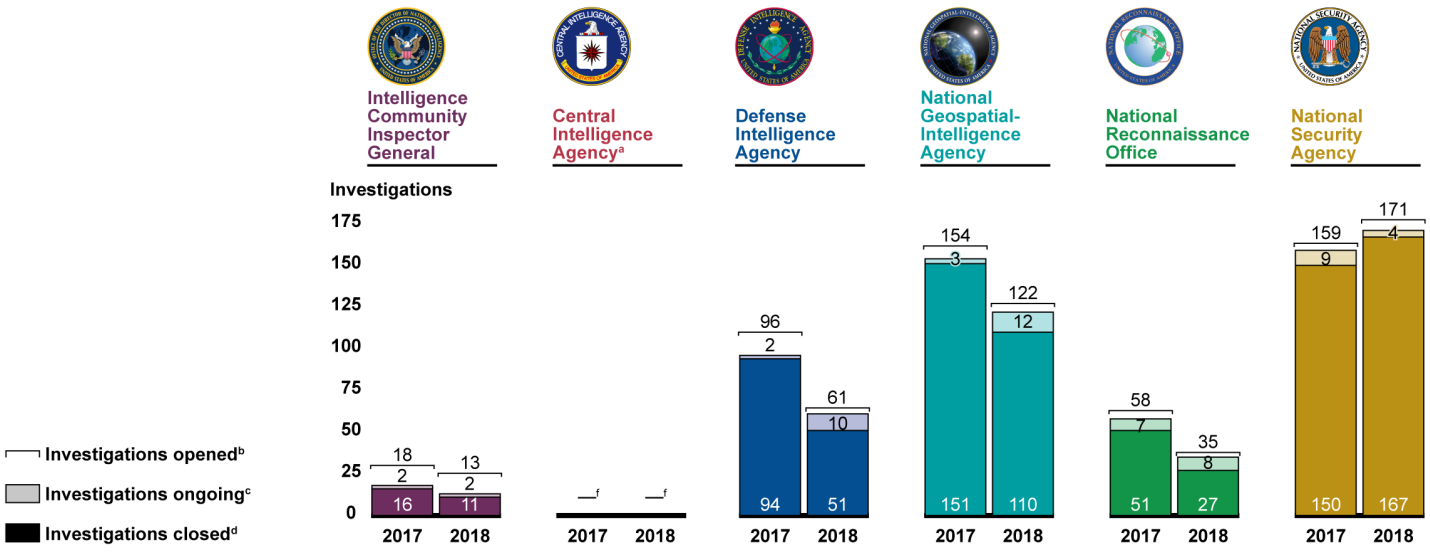
We found that the selected IC-element OIGs we reviewed collectively received 5,794 complaints from October 1, 2016, through September 30, 2018, and opened 960 investigations based on those complaints.[23] Of those 960 investigations, IC-element OIGs had closed 873 (about 91 percent) as of August 2019, with an average case time ranging from 113 days to 410 days to complete. Eighty-seven cases remained open as of August 2019, with the average open case time of 589 days across all six IC-element OIGs. The number of investigations at each of the IC-element OIGs varied widely, based on factors such as the number of complaints received by each IC-element OIG and the fact that each OIG makes its own determination on when to convert a complaint into an investigation. For example, CIA OIG procedures allow up to 120 days for preliminary investigative work to assess the credibility of a complaint, while DIA OIG procedures allow for only 10 days if the complaint involves activities in the

[23]The number of complaints presented here represent all complaints received by the IC-element OIGs, including complaints from sources other than whistleblowers. Specifically, according to IC-element OIG officials, some organizational units are required to report certain information to IC-element OIGs. For example, an IC element's security office may be required to notify the OIG in the event of a security incident that constitutes a potential violation of law, rule, or regulation.

continental United States.[24] Figure 2 depicts statistics for the number of investigations opened based on complaints received in fiscal years 2017 and 2018 and summary statistics for the time frames of these investigations, by fiscal year. Appendix II provides additional information on the number of complaints each IC-element OIG received in fiscal years 2017 and 2018, as well as the distribution of investigation time frames by IC-element OIG.

[24]Specifically, the CIA OIG's procedures allow 60 days of preliminary investigative work for all complaints, which may be extended to 120 days with approval of OIG management. The DIA OIG's procedures allow 30 days of preliminary investigative work for complaints that involve activities outside the continental United States.

Figure 2: Time Frame Statistics for Investigations of Complaints Received in Fiscal Years 2017 and 2018, as of August 2019



	Intelligence Community Inspector General		Central Intelligence Agency[a]		Defense Intelligence Agency		National Geospatial-Intelligence Agency		National Reconnaissance Office		National Security Agency	
	2017	2018	2017	2018	2017	2018	2017	2018	2017	2018	2017	2018
Average number of days to complete	251	177	410	228	292	183	195	159	306	234	128	113
Median number of days to complete	190	146	409	200	322	156	116	156	248	217	91	67
Maximum number of days to complete	547	384	939	409	757	428	790	583	833	484	604	421
Minimum number of days to complete[e]	6	6	8	41	9	12	0	0	31	119	0	1
Investigations completed in 180 days or fewer	8	7	6	7	32	28	92	71	16	9	109	123
Investigations completed in more than 180 days	8	4	25	7	62	23	59	39	35	18	41	44
Average number of days ongoing	776	485	934	444	746	383	833	380	838	473	817	499
Median number of days ongoing	776	485	943	422	746	353	853	333	874	469	785	520
Maximum number of days ongoing	837	553	1015	663	746	517	935	595	974	604	996	563
Minimum number of days ongoing	714	416	801	319	746	279	711	280	658	274	648	394

ICIG Inspector General of the Intelligence Community
CIA OIG Central Intelligence Agency Office of Inspector General
DIA OIG Defense Intelligence Agency Office of Inspector General
NGA OIG National Geospatial-Intelligence Agency Office of Inspector General
NRO OIG National Reconnaissance Office of Inspector General
NSA OIG National Security Agency Office of Inspector General

Source: GAO analysis of Intelligence Community-element data. | GAO-20-699

Note: IC-element OIGs may manage and track their case management data differently, as appropriate to each OIG's respective hotline and investigative processes. As a result, case times and number of investigations opened are not necessarily comparable across IC-element OIGs. Additionally, since we analyzed the status and time frames of investigations into complaints received in fiscal years 2017 and 2018 and some of the investigations have not been closed, the data presented here do not represent trends in case time frames between the two fiscal years.

[a]CIA OIG officials reported several factors that can contribute to longer case times for their investigations in comparison to other IC-element OIGs, including but not limited to issues pertaining to data access, austere personnel deployments, and use of certain investigative techniques and unique operational challenges.

[b]Figures provided for investigations represent the number of investigations that originated from complaints received in either fiscal year 2017 or fiscal year 2018. The actual number of investigations conducted, opened, and closed in each fiscal year may be higher, as we did not review data on investigations that originated from complaints received prior to fiscal year 2017.

[c]Case times for closed cases are calculated from the date each complaint was received to the date when the final report was signed. If no report or closure document was produced, we calculated the time from the date the complaint was received to the date when the case was formally closed or canceled.

[d]Case times for open cases are calculated from the date each complaint was received through the following dates: ICIG (August 9, 2019); CIA OIG (August 22, 2019); DIA OIG (July 11, 2019); NGA OIG (July 1, 2019); NRO OIG (June 26, 2019); NSA OIG (June 28, 2019).

[e]A value of "0" as the minimum number of days to complete an investigation denotes that an investigation was closed on the same day that the complaint was received.

[f]Specific details of the CIA OIG's investigation statistics were omitted because the CIA deemed that the information is sensitive.

IC-element OIG officials and investigators stated that the time needed to complete any given case can vary depending on a number of factors that can contribute to the complexity of a particular case, including the nature of the allegations, the responsiveness of the complainants and other involved parties, and the number of witnesses who must be interviewed. In particular, IC-element OIG officials and investigators noted that whistleblower reprisal and senior leader investigations can be among the most complicated cases to investigate, and these cases often require more time to complete than some other types of cases.[25] Additionally, IC-element OIG officials and investigators noted that case time frames are frequently driven by investigator workloads and the number of ongoing cases.

Four of Six IC-Element OIGs Have Timeliness Objectives for All Investigations, and Two Do Not

To help manage investigation time frames, four of the IC-element OIGs we reviewed—the CIA OIG, DIA OIG, NRO OIG, and NSA OIG—have a timeliness objective of 180-days or fewer for completing all types of investigations. Specifically, the CIA OIG's investigative procedures state that their objective is to complete investigations within 180 days. The DIA OIG's investigative procedures assign one of two different timeliness objectives, based on the priority of the investigation—120 days for high

[25]In addition to senior leader and reprisal cases, IC-element OIG officials and investigators stated that cases involving potential criminal activity, highly classified programs, or coordination with another federal OIG or the Department of Justice can also experience extended timelines.

priority investigations and 180 days for all others.[26] Additionally, the NRO OIG has a 180-day timeliness objective for all investigations in its draft investigations procedures. The NSA OIG has had a 180-day timeliness objective for whistleblower reprisal investigations in its whistleblower protection policy since 2015, and for completing all other investigations of average complexity in the performance objectives for the office's investigators, according to NSA officials, since at least 2015. Further, NSA OIG added a 180-day timeliness objective for all investigations to its investigative procedures in April 2020. Given the number of factors that can affect the time frames of OIG investigations, IC-element OIG officials stated that they believe any timeliness objective should allow for flexibility based on workloads and the specific circumstances of each case. However, these officials also stated that established timeliness objectives are nonetheless important for ensuring that investigations are conducted efficiently.

The ICIG's and NGA OIG's procedures state that investigations should be conducted and reported in a timely manner. Additionally, the NGA OIG's investigations procedures include time frames for completing some steps of its investigative process, such as completing the report of a preliminary investigation. CIGIE's *Quality Standards for Investigations* states that investigations must be conducted in a timely, efficient, thorough, and objective manner. Additionally, *Standards for Internal Control in the Federal Government* states that management should define objectives clearly to enable the identification of risks, which typically involves defining the time frames for completing objectives in specific, measurable terms. However, other than those prescribed by statute, neither the ICIG nor the NGA OIG has established specific, measurable timeliness objectives for completing investigations in their policies and investigative procedures. These two IC-element OIGs did not provide an explanation for not including the timeliness objectives as part of their policies and procedures. Establishing specific timeliness objectives in policies and procedures for all investigations, other than those already prescribed by statute, could help the ICIG and NGA OIG to conduct and report on their investigations in a timely manner and could enable them to inform potential whistleblowers of the time frames for conducting investigations.

[26]DIA's procedures define high priority investigations as those involving senior officials or national security, those affecting the seat of government or immediately affecting DIA effectiveness or operational capability, joint investigations, and investigations directed by the director or Inspector General of DIA.

Each IC-Element OIG Has Implemented Some Quality Assurance Processes, but Some OIGs Do Not Regularly Update Guidance or Conduct Routine Quality Assurance Reviews

All of the IC-element OIG whistleblower protection programs we reviewed had implemented some quality assurance standards and processes, but the extent to which they had implemented processes to maintain guidance, conduct routine quality assurance reviews, and plan investigations varied. Further, all IC-element OIGs have processes in place to help ensure that their investigations align with CIGIE quality standards related to matters such as adhering to ethical principles, maintaining quality assurance for investigations, and exercising due professional care. However, most of the six IC-element OIGs we reviewed lack processes to regularly update their procedures for investigations. In addition, while some IC-element OIGs have conducted internal or external reviews of their investigative units, only the CIA OIG routinely submits itself to external quality assurance reviews. Finally, five IC-element OIGs routinely use documented investigative plans, but the NRO OIG does not.

All Six Selected IC-Element OIGs Have Implemented Quality Assurance Processes

Each of the selected IC-element OIGs has incorporated CIGIE standards to some degree into its operations by, for example, including codes of conduct and ethical and professional standards derived from CIGIE in its guidance. Moreover, each of the IC-element OIGs has implemented at least some quality assurance processes to help ensure that its investigative activities align with CIGIE standards. For example:

- Each of the IC-element OIGs we reviewed has processes in place to review case files and investigative reports.
- Each of the IC-element OIGs we reviewed has assigned specific quality assurance responsibilities to supervisors in its investigations division. These quality assurance responsibilities include reviewing reports of investigation and case files to ensure that all required investigative steps are completed and appropriately documented, and that the investigations' conclusions are legally sound and supported by appropriate evidence. In the case files we reviewed, we found documentation showing that supervisory review had occurred in all 28

cases and that legal review had occurred or was not required in 26 of the 28 cases.[27]

- The CIA OIG requires that investigators link all factual statements presented in a report to evidence collected during the investigation. The CIA OIG management then assigns a second investigator who was not involved in the investigation to review the report to verify factual data and determine whether the findings are supported by the case file documentation.

Furthermore, all of the 39 investigators we interviewed were familiar with their respective organizations' quality assurance processes and stated that they were confident that the processes prevent both institutional and individual bias from influencing investigations.

In addition to guidance and report review processes, some IC-element OIGs have additional measures to facilitate quality assurance. For example, all six IC-element OIGs conduct monthly or weekly progress reviews, as appropriate, for each investigation or for each of their priority cases.[28] IC-element OIG managers stated that investigators use these progress reviews to brief management—which can include the Inspector General and Deputy Inspector General—on the status of investigations. For preliminary inquiries, progress reviews may also be used to determine whether an inquiry should be converted to a formal investigation. In addition to progress reviews, most of the IC-element OIGs we reviewed—specifically the ICIG, CIA OIG, NGA OIG, NRO OIG, and NSA OIG—have developed standardized case closing checklists or memorandums that may be used to help OIG managers and investigators

[27]Generally, all IC-element OIGs we reviewed require legal sufficiency reviews or consultation with the IG's legal counsel at certain points in the investigative process. The NSA OIG did not require a legal review in one unsubstantiated case, because it was a summary report for an unsubstantiated matter in which the subject had resigned. The NSA OIG also provided data indicating that legal reviews had occurred in three additional unsubstantiated cases, but we were unable to identify documentary evidence of a legal review for these cases. Additionally, we did not identify any documentation of a legal review for one CIA OIG case; in that case, a limited amount of investigative work was required to show that the allegations were not credible. The one case file that we reviewed at the ICIG was for an External Review Panel, and not an original investigation. As such, we did not analyze it against this standard.

[28]Some IC-element OIGs have developed explicit criteria to identify priority investigations. For example, the CIA OIG, NGA OIG, NRO OIG, and NSA OIG have each identified senior official misconduct, reprisal, and criminal cases, among other categories, as high priority investigations. For these high priority cases, the respective Inspectors General and Deputy Inspectors General participate in routine progress reviews. DIA OIG officials told us that they also increase the frequency of such reviews for investigations that their Inspector General has identified as highly sensitive.

ensure that required investigative work has been fully documented, and that case files are complete before closure.

Two of the Six Selected IC-Element OIGs Have Recently Updated Their Investigation Procedures, but Four of the Six Do Not Do So Regularly

The extent to which IC-element OIGs regularly update their investigation procedures to account for statutory and other policy changes varied. Specifically, the NGA OIG and NSA OIG have each implemented processes to update their respective investigative procedures regularly. NGA OIG officials stated that their schedule is to formally publish revisions to the investigations manual every 5 years—and did so in 2013 and 2018—but that they collect and maintain all revisions to the procedures annually between the formal updates. NGA OIG officials also stated that one investigator in their organization has been assigned responsibility to annually collect revisions to the NGA OIG investigation manual—including coordinating potential updates with both investigative staff and the NGA IG's legal counsel—to ensure that the procedures in the manual align with investigator needs and any changes in legal requirements. The NSA OIG also has a process to regularly update its procedures. Specifically, the NSA OIG updated its standard operating procedures for investigations repeatedly from 2015 through 2019, and updated its procedures for intake in 2016 and 2018. Both of these documents include specific guidance for whistleblower reprisal cases.

However, while three of the IC-element OIGs we reviewed have updated their policies since Presidential Policy Directive 19 was signed in 2012, recent changes to statute extending whistleblower reprisal protections to IC contractors, subcontractors, grantees, and subgrantees have not yet been incorporated.[29] It has taken several years for the ICIG, CIA OIG, and DIA OIG to make updates and revisions to their procedures to incorporate changes to statute or other policy changes, which the ICIG and CIA OIG have still not finalized.

- **ICIG:** ICIG officials acknowledged that their 2014 investigations manual is outdated and stated that they are currently working to update it. Officials stated during our review that they planned to finalize this update by the end of fiscal year 2019, but they did not meet this time frame. The ICIG is currently planning to complete these revisions by the end of calendar year 2020.
- **CIA OIG:** According to CIA OIG officials, they last updated their investigations procedures in July 2015. CIA OIG officials stated in September 2019 that they have several amendments and revisions

[29]FISA Amendments Reauthorization Act of 2017, Pub. L. No. 115-118, § 110 (2018).

awaiting approval pending the completion of an ongoing review by the CIA OIG's deputy counsel. As of mid-March 2020, CIA OIG had not completed this revision, but officials stated that they expected to finalize it by the end of the month.

- **DIA OIG:** The DIA OIG updated its standard operating procedures for investigations in 2017 and updated its supplemental procedures for whistleblower reprisal investigations in 2018. Although these procedures include whistleblower protections that were mandated by Presidential Policy Directive 19 and the Intelligence Authorization Act of 2014 in 2012 and 2014, respectively, it took several years for the DIA OIG to complete the updates.

The time frames needed to finalize these revisions were prolonged in part because the ICIG, CIA OIG, and DIA OIG have not established processes to regularly update their procedures. Additionally, ICIG officials told us that they plan to complete their revisions by the end of calendar year 2020.

NRO OIG officials stated that they last finalized their investigations manual in 2010, before Presidential Policy Directive 19 was signed; only one of the five NRO OIG investigators we interviewed cited this manual as a source of guidance that they use to conduct investigations. According to NRO OIG officials, their office has had a draft manual in development since a number of needed revisions were identified in 2013, but it has not been finalized. The NRO OIG provides investigators with 25 operating instructions that generally provide procedures for select investigative activities, such as referring evidence of potential criminal activity and handling NRO personnel and security records. Additionally, one operating instruction provides investigative procedures for time and attendance cases and contractor labor mischarging cases. However, the NRO OIG's operating instructions do not provide guidance on investigative standards or the overall investigative process for all cases. NRO OIG officials stated that they are working to finalize the manual, but that competing priorities have prevented them from completing several prerequisites. Specifically, NRO OIG officials stated that they did not plan to finalize the manual until completing both an internal and an external quality assurance review. NRO OIG officials stated that they estimated these steps would be completed by the end of calendar year 2019. However, NRO OIG officials stated that they have not established a time frame for finalizing the manual once the prerequisites are complete, and that they have not established a process to regularly update the manual once it has been finalized.

CIGIE's *Quality Standards for Investigations* states that due professional care must be used in conducting investigations, and that organizations should facilitate due professional care by establishing written investigative policies and procedures via handbooks, manuals, or similar mechanisms that are revised regularly according to evolving laws, regulations, and executive orders. Additionally, *Standards for Internal Control in the Federal Government* states that management should implement and document controls through policies and should remediate identified internal control deficiencies on a timely basis.[30] This can include regularly reviewing procedures to ensure continued relevance and effectiveness. By establishing processes to regularly update their procedures, the ICIG, CIA OIG, DIA OIG, and NRO OIG could better ensure that their policies and procedures will remain consistent with evolving laws, regulations, Executive Orders, and CIGIE standards. *Standards for Internal Control in the Federal Government* also states that management should define objectives clearly to enable the identification of risks and define risk tolerances, which typically includes clearly defining the time frames for completing an objective.[31] Establishing time frames for completing ongoing updates of reviews of their investigations procedures would help ensure that ICIG, CIA OIG, and NRO OIG staff have documented and current guidance needed to conduct investigations.

Some IC-Element OIGs Have Conducted Internal or External Reviews of Their Investigations Units, but These Reviews Are Generally Not Routine

Several of the IC-element OIGs we reviewed provided information on their plans and efforts to conduct internal or external quality assurance reviews of their investigations units, but none of them routinely submits its investigations division to both kinds of reviews. CIGIE's *Quality Standards for Federal Offices of Inspector General* requires OIGs to establish and maintain a quality assurance program. The standards further state that internal and external quality assurance reviews are the two components of an OIG's quality assurance program, which is an evaluative effort conducted by reviewers independent of the unit being reviewed to ensure that the overall work of the OIG meets appropriate standards. CIGIE standards state that internal quality assurance reviews are conducted by internal OIG staff who are external to the unit being reviewed, and that external quality assurance reviews are conducted by independent organizations not affiliated with the OIG being reviewed. CIGIE has developed guidance for organizations to use when conducting quality assurance reviews of OIG investigations divisions, known as *Qualitative*

[30]GAO-14-704G.

[31]GAO-14-704G.

Assessment Review Guidelines for Investigative Operations of Federal Offices of Inspector General.[32]

Internal Quality Assurance Reviews

The DIA OIG established a designated quality assurance branch in 2018 that is external to the audits, evaluations and inspections, and investigations divisions. The quality assurance branch completed a series of targeted internal quality assurance reviews of DIA's investigations division in 2018.

None of the other five IC-element OIGs has conducted routine internal quality assurance reviews, which are a key component of an OIG's quality assurance program. Some IC-element OIGs we reviewed stated that they have been focused on other efforts and have not conducted internal quality assurance reviews, while others were either not familiar with internal reviews or provided examples of internal reviews that do not align with CIGIE's definition of an internal quality assurance review. Specifically:

- **ICIG** reported that it has not conducted an internal quality assurance review and it has not been a standard practice of either current or previous ICIG leadership to do so. ICIG officials stated they believe it is currently premature to initiate an internal quality assurance review due to a number of ongoing changes that include hiring more investigative staff and developing and implementing new processes and procedures. These officials stated in June 2019 that the ICIG may be in an appropriate position to conduct an internal quality assurance review once it has filled its open vacancies, completed revisions to its investigations procedures, and trained both incoming and existing staff on new and revised policies and procedures.
- **CIA OIG** completed a self-inspection of its investigation program in 2019. For this inspection, a manager in the investigations division reviewed 14 closed investigative case files for alignment with the CIA OIG's investigative procedures and CIGIE standards. However, the self-inspection does not align with CIGIE's definition of an internal quality assurance review in that it was not conducted by OIG personnel who are external to the investigations division.
- **NGA OIG** reported that it has completed several routine internal reviews. Specifically, the NGA OIG stated that OIG personnel from outside of the investigations division conducted reviews of that

[32]CIGIE, *Qualitative Assessment Review Guidelines for Investigative Operations of Federal Offices of Inspector General* (July 18, 2017).

division's information security and internal control programs in April 2019 and May 2019, respectively. However, these reviews did not evaluate the investigations division against CIGIE's qualitative assessment review guidelines, and they were not designed to evaluate the aspects of OIG operations described in CIGIE quality standards for federal OIGs.

- **NRO OIG** officials stated that they completed a self-assessment of their investigations division in June 2019. However, this review did not align with CIGIE's definition of an internal quality assurance review in that it was not conducted by OIG staff who are external to the unit being reviewed. NRO OIG officials also reported that they have no record of having ever completed an internal quality assurance review. According to one NRO OIG official, they intend to conduct internal quality assurance reviews every 2 to 3 years, but have not made specific plans to do so.
- **NSA OIG** officials stated that their investigations division did not have formal internal quality assurance procedures but the OIG is expanding its quality control program to encompass the entire OIG. Going forward, according to the officials, NSA OIG is planning to develop internal quality assurance procedures for all divisions, including the investigations division, which are consistent with CIGIE standards.

External Quality Assurance Reviews

One IC-element OIG conducts routine external quality assurance reviews. Two other IC-element OIGs have plans to conduct external quality assurance reviews in the future, but these reviews have not been routine in nature. Specifically:

- **CIA OIG** routinely submits its investigations division to an external quality assurance review every 3 years, and the most recent reviews occurred in 2014 and 2017; neither of the reviews identified deficiencies, but both made observations on potential improvements. The CIA OIG investigations division's next external review is planned for 2021.
- **DIA OIG** stated in May 2019 that it was starting the planning process for an external quality assurance review of its investigations division to commence after the DIA OIG completes its transition to a new case management system. As of December 2019, DIA OIG officials stated that the planned start date for the external review would be in the third or fourth quarter of fiscal year 2020. According to a DIA OIG official, they have not previously conducted an external quality assurance review of the investigations division.

- **NRO OIG** officials stated that they have plans to initiate an external quality assurance review of their investigations division in 2020, conducted by the CIA OIG. The NRO OIG reported that the investigations division's most recent external quality assurance review was completed more than 9 years ago, in June 2010; the review did not identify any deficiencies in NRO OIG's investigative operations, but it made observations.

The investigations divisions of two IC-element OIGs—the ICIG and NGA OIG—have not been externally reviewed, and NSA OIG's investigations division has not been externally reviewed since at least 2013. Additionally, officials from these OIGs said they do not currently have any plans to undergo external quality assurance reviews in the future. Officials from the ICIG told us that they have not initiated an external quality assurance review of their investigations division because, similar to internal quality assurance reviews, doing so has not been a standard practice of current or previous leadership. Additionally, ICIG officials believe it is currently premature to initiate an external review due to their having ongoing initiatives, but they acknowledged that they could do so once these initiatives have been completed. We believe that it would be reasonable at that point for the ICIG to begin conducting internal and external quality assurance reviews of its investigations division. Officials from both the NGA OIG and the NSA OIG acknowledged that external quality assurance reviews would benefit their investigations units. Specifically, the NGA OIG stated that external quality assurance reviews would help them share best practices from other federal OIGs, and the NSA OIG stated that the reviews would help them identify areas for improvement. The NSA OIG also reported that external quality assurance reviews provide an independent perspective on operations. Despite these benefits, neither the NGA OIG nor the NSA OIG has plans to initiate an external quality assurance review of their investigations divisions in the future, although the NSA OIG stated that it will be a priority for the NSA OIG's recently hired Assistant Inspector General for Investigations to plan one in the future.

CIGIE's *Quality Standards for Federal Offices of Inspector General* requires that each federal OIG shall establish and maintain a quality assurance program to ensure that work performed adheres to established OIG policies and procedures; meets established standards of performance, including applicable professional standards; and is carried out economically, efficiently, and effectively. CIGIE quality standards further state that quality assurance programs consist of an evaluative effort conducted by reviewers independent of the unit being reviewed, to

ensure that the overall work of the OIG meets appropriate standards. CIGIE standards acknowledge that the nature and extent of an OIG's quality assurance program depends on a number of factors, including the OIG's size, the nature of its work, its organizational structure, and appropriate cost and benefit considerations. As such, the standards recognize that the quality assurance programs established by different OIGs can vary. However, CIGIE standards state that these efforts are to include internal quality assurance reviews at a minimum, and the standards strongly recommend that they include external quality assurance reviews. According to the standards, external quality assurance reviews provide OIGs with added assurance regarding their adherence to prescribed standards, regulations, and legislation through a formal objective assessment of OIG operations.

While three of the IC-element OIGs we reviewed—the CIA, DIA, and NRO OIGs—have either internal or external quality assurance reviews planned or underway, none of these IC-element OIGs routinely conducts both kinds of reviews. That is because their quality assurance programs do not include both kinds of reviews that meet CIGIE's criteria. Developing quality assurance programs that incorporate both types of reviews, as appropriate, could help ensure that the IC-element OIGs adhere to OIG procedures and prescribed standards, regulations, and legislation, as well as identify any areas in need of improvement.

All six IC-element OIGs in our review said that their investigations divisions would benefit from conducting external quality assurance reviews. However, both the NGA OIG and the NSA OIG stated that they have been unable to schedule external quality assurance reviews because of personnel constraints, such as difficulty in identifying other OIGs that have sufficient staff with appropriate clearances to perform those reviews. Additionally, officials from the NSA OIG stated that they have attempted to coordinate with the ICIG to schedule external reviews, but that the ICIG did not have a process in place to identify cleared staff and facilitate external peer reviews for IC-element OIGs. As previously discussed, the ICIG has a coordination role among the IC-element OIGs. ICIG officials stated that their office's coordination role includes providing services to other IC-element OIGs to facilitate external quality assurance reviews of their audit and inspection divisions, but the ICIG does not currently provide these services to the OIGs' investigations divisions. ICIG officials stated that they have considered providing this service but have not yet done so, as they were focused on their ongoing hiring efforts and policy updates. Establishing a process to facilitate external quality assurance reviews for the IC-element OIGs' investigations divisions could

further the ICIG's coordination role and better position the other IC-element OIGs to include external quality assurance reviews as a component of a strong quality assurance program.

Five of Six IC-Element OIGs Require Investigative Plans, but the NRO OIG Does Not Routinely Use Documented Investigative Plans to Establish Case-Specific Priorities

The ICIG, CIA OIG, DIA OIG, NGA OIG, and NSA OIG all require their investigators to use documented investigative plans to identify and prioritize the investigative work they plan to complete in the course of an investigation. Each of these OIGs also provides its investigators with plan templates that are designed to align with their respective applicable regulations and investigative procedures. We identified documented investigative plans in each of the case files we reviewed for four of these five IC-element OIGs.[33] However, NRO OIG officials stated that their investigators do not routinely use documented investigative plans or otherwise establish case-specific priorities for investigations. We reviewed the case files for two whistleblower reprisal and two senior leader investigations completed by the NRO OIG from October 1, 2016, through March 31, 2018. Although these types of cases can be some of the most significant and highest-priority investigations that OIGs investigate, the NRO OIG did not use a documented investigative plan in any of these cases.

All of the NRO OIG investigators we interviewed stated that, in their belief, either investigative plans are not necessary for experienced investigators; investigative plans are needed only in the most complex cases; or they do not use investigative plans because they set priorities informally with supervisors. NRO OIG managers stated that they see value in documented investigative plans to ensure that all investigative activities are completed in a timely manner, and that they encourage investigators to use documented investigative plans when appropriate, such as for highly complex investigations. Additionally, the NRO OIG has created an investigative plan template to help investigators develop plans for investigations if they choose to do so. NRO OIG managers stated that it is ultimately up to the individual investigators to plan their work and decide whether to use a documented investigative plan.

CIGIE *Quality Standards for Investigations* requires that case-specific priorities must be established and objectives developed to ensure that tasks are performed efficiently and effectively. CIGIE's standards further state that this may best be achieved, in part, by preparing case-specific

[33]The one ICIG case file we reviewed was for an External Review Panel. As such, an investigative plan was not required.

plans and strategies. Although NRO OIG managers acknowledge the value of using investigative plans and NRO OIG officials stated that they encourage investigators to use such plans when appropriate, the NRO OIG does not routinely use documented investigative plans for all investigations because it has not established a requirement to do so. The ICIG, CIA OIG, DIA OIG, NGA OIG, and NSA OIG have all established such a requirement for their investigators to use investigative plans as a mechanism for meeting the CIGIE standard. Establishing a requirement that investigators use documented investigative plans for all investigations could better position NRO OIG management to oversee investigations and ensure that investigative steps are prioritized and performed efficiently and effectively.

Investigators Attend a Variety of Training Courses, but Three of Six IC-Element OIGs Have Not Established Training Requirements in a Documented Plan

The 39 IC-element OIG investigators we interviewed stated that they take a variety of relevant training courses, and investigators from all six IC-element OIGs stated that managers are supportive of investigators' training requests. However, three IC-element OIGs have not established training requirements for their investigators that are linked to the requisite knowledge, skills, and abilities, appropriate to their career progression, and part of a documented training plan.[34] Each of the selected IC-element OIGs encourages or requires its new investigators to attend some basic courses relevant to their position. For example, investigators from all six IC-element OIGs stated that they had attended either criminal investigator training provided by the Federal Law Enforcement Training Center or inspector general investigations training provided by CIGIE. In addition to these basic investigator training courses, these investigators also told us that they take specialized training, such as digital forensics courses or certified fraud examination training.

It is the responsibility of each investigator at all six IC-element OIGs to identify his or her own training needs and to discuss those with his or her supervisor annually. Each of the six IC-element OIGs we reviewed either requires or offers individual development plans to investigators, which can be used to manage each investigator's training and career development.[35] While these plans are designed to meet the needs of

[34]These 39 investigators were all of the currently employed IC-element OIG investigators who had experience in conducting reprisal or senior leader investigations.

[35]An individual development plan is a written plan, cooperatively prepared by the employee and his or her supervisor, that outlines the steps the employee will take to develop knowledge, skills, and abilities in building on strengths and addressing weaknesses as he or she seeks to improve job performance and pursue career goals.

individual investigators, they are not necessarily linked to a consistent set of professional proficiencies for investigators.

Three of the IC-element OIGs we reviewed—the CIA OIG, DIA OIG, and NGA OIG—provided examples of training plans or approaches that are linked to the requisite knowledge, skills, and abilities, appropriate to their career progression, and part of a documented training plan consistent with CIGIE's standard for investigator training.

- **CIA OIG:** The CIA OIG's investigation procedures state that all investigators are to possess the necessary knowledge, skills, and abilities for their assignments and developmental level, and that they are to conform to training qualifications outlined in CIGIE's *Quality Standards for Investigations*. To ensure that investigators meet this requirement, the CIA OIG's investigation procedures includes a training matrix that discusses both required and recommended trainings at each developmental level to help investigators develop core competencies described in CIGIE standards as they progress through their careers. Additionally, the procedures identify two basic training courses that are required for all new investigators: the Criminal Investigator Training Program offered by the Federal Law Enforcement Training Center, or equivalent, and the Inspector General Investigator Training Program offered by CIGIE.[36] The CIA OIG also requires that new investigators attend an orientation course designed to familiarize them with OIG investigative authorities, policies, and procedures, as well as with CIA components that frequently interact with the CIA OIG's investigations division. After completion of the mandatory basic training courses, CIA OIG investigators periodically receive additional refresher training, such as victim and witness awareness, legal refresher courses, and blood-borne pathogen training.
- **DIA OIG:** The DIA OIG has documented a formal career path guide to help ensure systematic, progressive training for all OIG employees. The guide defines the key knowledge, skills, and abilities associated with applicable competencies for all OIG employees generally, for career fields and specialties—including investigators—more specifically, and at different stages of career progression for each career specialty. The career path guide also includes lists of recommended training courses for investigators at each phase of their

[36]The CIA OIG's investigations manual states that new investigators who meet certain requirements for prior investigative experience may complete the Transitional Training Program offered by CIGIE in lieu of the Inspector General Investigator Training Program.

careers. DIA OIG officials stated that their career path guide represents the results of a job analysis that redefined the competencies and performance standards for different career fields and grades. These officials stated that they use the career path guide to ensure that their investigator training is consistent with the DIA OIG's competencies for investigators and CIGIE's *Quality Standards for Investigations*. In addition to the guidance in the career path guide, the DIA OIG also requires that all investigators complete the DOD OIG's whistleblower reprisal training. DIA OIG officials stated that their ongoing internal quality assurance review and planned external quality assurance review will also assess investigator training needs.

- **NGA OIG:** The NGA OIG finalized a career resource guide in August 2019. NGA OIG officials stated that the guide is intended as a singular reference to help all OIG employees acquire, maintain, and grow the education, experience, and exposure they need to enable the OIG mission and manage their own professional development. The guide identifies for NGA OIG employees—broken out by work role, including investigators—the knowledge, skills, and abilities that they should achieve at each level of career progression, and it provides relevant training recommendations for each stage. For example, the guide provides information on a variety of courses, certifications, and professional skills appropriate to each career level that meet NGA OIG's educational requirements for its investigators. Additionally, NGA OIG has developed a training and development plan for investigators who are hired into the OIG with relevant outside career experience. In addition to these resources, the NGA OIG's investigation procedures state that investigators must maintain proficiency in investigative skills and in their own areas of expertise, and that investigators will attend a combination of internal and external courses to maintain and upgrade their professional skills and knowledge of the NGA OIG's processes. The NGA OIG's procedures also include a list of available training courses for investigators to use as a reference.

Although all of the investigators we spoke with at all six IC-element OIGs received training relevant to performing their daily responsibilities, the extent to which the ICIG, NRO OIG, and NSA OIG provide an approach to training that consistently supports investigators' required professional proficiencies varies, as described below:

- **ICIG:** ICIG officials stated that they have developed human capital processes, competencies, and trainings that comply with CIGIE's quality standards. The ICIG's 2014 investigations procedures describe the basic qualifications and responsibilities for ICIG investigators and

include suggested training courses that investigators may attend. The procedures state that investigators are individually responsible for ensuring that they obtain the required 20 hours of training each calendar year, and that the ICIG should designate one employee to act as a training coordinator to facilitate training. Additionally, ICIG officials stated that all new investigators are required to attend CIGIE's inspector general investigations training, attend DOD OIG's whistleblower reprisal course, and complete coursework required to obtain certification from the Association of Fraud Examiners. Further, ICIG officials said they have developed a draft career path and training plan to help investigators identify courses that will enhance their skills and subject matter expertise as their careers advance. This plan includes required and suggested training, including training recommended or required at each phase of investigators' careers. However, the ICIG's existing procedures do not include a progressive training plan or requirements for an investigator's career development. Since the ICIG is still in the process of updating its procedures and has not finalized its draft training plan, we could not determine whether the final version of those documents will include a systematic, progressive, and documented training plan that includes specific training linked to the requisite knowledge, skills, and abilities to fulfill an investigator's responsibilities.

- **NRO OIG:** NRO OIG officials stated that they continuously monitor each employee's experience, expertise, and training to ensure that investigators are positioned to address the myriad issues that arise in the course of performing their duties. Additionally, NRO OIG officials stated that newly assigned investigators are expected to attend either criminal investigator training provided by the Federal Law Enforcement Training Center or inspector general investigations training provided by CIGIE within their first year if they do not have prior training or experience. The NRO OIG also provides investigators with a sample training plan, but it does not require investigators to follow the sample plan. NRO OIG officials told us that managers may consider the needs of the individual employee, office requirements, and available resources as they formulate each employee's training plan for the coming year. In addition, the NRO OIG provides training guidance on an internal website that incorporates information from CIGIE standards and states that a continuous career development program should be established. However, neither the sample training plan nor the NRO OIG's training guidance links specific training to the requisite knowledge, skills, and abilities to fulfill an investigator's responsibilities as his or her career progresses.

- **NSA OIG:** NSA OIG officials told us that all new investigators—including those with prior experience—are required to attend either basic criminal investigator training provided by the Federal Law Enforcement Training Center or basic inspector general investigations training provided by CIGIE within their first year. The NSA OIG also encourages investigators to take the DOD OIG's whistleblower reprisal course at least once. After completing one of the basic trainings, NSA OIG investigators are each expected to attend at least one external training event per year, within the constraints of the NSA OIG's training budget. NSA OIG's procedures also state that investigators should submit an individual development plan and document satisfactory completion of education and training to the OIG training officer, who NSA officials stated is an investigator designated to assist other investigators in identifying potential training options. According to NSA OIG officials, individual training is a component of each investigator's performance plan. In addition to formal training, NSA officials stated that each new NSA OIG investigator is paired with an experienced investigator who acts as a mentor and provides on-the-job training tailored to the skills and experience of each new employee. However, beyond the initial training requirements listed above, the NSA OIG does not have a documented plan or other guidance that links specific knowledge, skills, abilities, and trainings to an investigator's career progression. NSA officials stated that they are in the process of hiring a new Assistant Inspector General for Investigations, and that one of his or her top priorities will be to examine the investigations division's training requirements and procedures.

CIGIE's *Quality Standards for Investigations* requires that individuals assigned to conduct investigative activities must collectively possess professional proficiencies for tasks required. In order to meet this requirement, the standards state that OIGs should establish appropriate avenues for investigators to maintain the necessary knowledge, skills, and abilities to perform investigative activities, and that training should be part of a systematic, progressive, and documented plan. Moreover, *Quality Standards for Investigations* states that the training of an investigator should be a continuing process and that a continuous career development program should be established to provide the proper preparation, training, and guidance to develop trainees into professionally qualified investigators and supervisors. Additionally, *Standards for Internal Control in the Federal Government* states that management of an entity should demonstrate a commitment to recruit, develop, and retain competent individuals. Management may also establish expectations of

competence for all personnel through policies within the entity's internal control system. The Standards also state that management should define objectives clearly to enable the identification of risks and define risk tolerances, including how those objectives and risk tolerances affect the expectations of competence for its personnel. Documented training plans are an example of a control activity that can be implemented through an agency's policies and procedures.

The CIA OIG, DIA OIG, and NGA OIG have documented in their investigation procedures or career guides an approach that links necessary knowledge, skills, and abilities to a systematic, progressive training plan. The ICIG, NRO OIG, and NSA OIG, however, do not have training plans or other documents that systematically link the requisite knowledge, skills, and abilities and training requirements to an investigator's career progression, in part because they view their current efforts as sufficient. Establishing training plans that include this information would provide greater assurance to the ICIG, NRO OIG, and NSA OIG that their investigators collectively possess professional proficiencies for the tasks required throughout their entire career progression.

Most Selected IC-Element OIGs Consistently Met Congressional Notification and Reporting Requirements, but Not All of Them Always Documented Notifications to Complainants

Most of the IC-element OIGs we reviewed consistently met congressional notification and reporting requirements for the investigations and semiannual reports we reviewed. Additionally, regarding the requirement for the defense IC-element OIGs to notify the DOD OIG of credible allegations, the DOD OIG entered into a memorandum of understanding with the DIA OIG, NGA OIG, NRO OIG, and NSA OIG in July 2019. The memorandum of understanding is intended to clarify aspects of the relationship between the DOD OIG and the defense intelligence OIGs, enhance execution of their respective missions, and strengthen cooperation and collaboration among the DOD OIG and the defense intelligence OIGs. Further, while all IC-element OIGs we reviewed have policies or investigation procedures that require them to provide information to the complainant about the results of any investigation into allegations of whistleblower reprisal made by them, three did not consistently document these notifications in reprisal investigations cases we reviewed.

Most Selected IC-Element OIGs Consistently Met Congressional Notification and Reporting Requirements for Closed Cases and Semiannual Reports Reviewed

Most of the selected IC-element OIGs consistently met congressional notification and reporting requirements for the investigations and semiannual reports we reviewed. Various statutes establish requirements for the IC-element OIGs to report information about certain investigative activities to Congress. These requirements include notifying Congress of investigations that meet specified criteria and providing Congress with certain information in semiannual reports.

Notifications for CIA Senior Leadership Cases

Section 3517 of Title 50, United States Code, requires that the CIA OIG immediately notify the congressional intelligence committees whenever an investigation is conducted involving senior leaders of the CIA.[37] We reviewed the case files of all investigations closed by the CIA OIG in which this requirement applied during the time frame of our review—October 1, 2016, through March 31, 2018—and found documentation showing that CIA notified Congress as required by statute in all cases.[38]

Notifications of Complaints Involving Urgent Concern

The Intelligence Community Whistleblower Protection Act of 1998 requires that the heads of each IC element shall notify congressional intelligence committees of all allegations of urgent concern that their respective OIGs have received and found to be credible.[39] IC-element

[37]Specifically, the CIA IG is to immediately notify and submit a report to the congressional intelligence committees in the event that an investigation, inspection, or audit carried out by the Inspector General should focus on any current or former CIA official who holds or held a position in the agency that is subject to appointment by the President, by and with the advice and consent of the Senate, including such a position held on an acting basis; or holds or held the position in CIA, including such a position held on an acting basis, of Deputy Director; Associate Deputy Director; Director of the National Clandestine Service; Director of Intelligence; Director of Support; or Director of Science and Technology. See 50 U.S.C. § 3517(d)(3)(B).

[38]Specific details of the CIA OIG's investigation statistics were omitted because the CIA deemed that the information is sensitive.

[39]The Intelligence Community Whistleblower Protection Act of 1998, Pub. L. No. 105-272, §§ 701-702 (1998) and codified at section 8H of Appendix, Title 5, U.S. Code defines "urgent concern" as any of the following: (1) a serious or flagrant problem, abuse, violation of law or Executive order, or deficiency relating to the funding, administration, or operations of an intelligence activity involving classified information, but does not include differences of opinions concerning public policy matters; (2) a false statement to Congress, or a willful withholding from Congress, on an issue of material fact relating to the funding, administration, or operation of an intelligence activity; or (3) an action, including a personnel action described in section 2302(a)(2)(A) of Title 5, United States Code, constituting reprisal or threat of reprisal prohibited under the statute in response to an employee's reporting an urgent concern.

OIG officials stated that complaints alleging an urgent concern are not common, but that senior OIG management or the legal counsels of the Inspectors General are generally responsible for notifying Congress when they do occur. Of the 27 investigations we reviewed, none involved a complaint or information of an urgent concern under the statute.

Semiannual Reports

Section 5 of Title 5, Appendix, United States Code, and sections 3517 and 3033 of Title 50, United States Code, contain general requirements for IC-element OIGs to notify Congress of certain OIG activities in semiannual reports. These statutes require OIGs to report to Congress certain information about audits, inspections, investigations, and peer reviews.[40] Section 5 of Title 5, Appendix, United States Code, establishes the requirements for semiannual reports for the OIGs of DIA, NGA, NRO, and NSA. Section 5 requires specific information on OIG investigative activities, including statistical tables identifying the number of referrals for prosecution and their results, a report on each investigation involving an allegation of misconduct against a senior government employee, and a detailed description of any instance of whistleblower retaliation. Table 2 shows the record of compliance of the DIA, NGA, NRO, and NSA OIGs with the requirements for semiannual reports.

Table 2: Defense Intelligence Community Office of Inspector General (OIG) Compliance with Selected Statutory Requirements for Semiannual Reports, Fiscal Years 2017 and 2018

Section 5 Requirement	Defense Intelligence Agency (DIA)	National Geospatial-Intelligence Agency (NGA)	National Reconnaissance Office (NRO)	National Security Agency (NSA)
Statistical tables showing total number of investigative reports, criminal referrals, and results of past referrals	✓	✓	✓	✓
Reports on each investigation conducted involving a senior government employee where allegations of misconduct were substantiated	✓	✓	✓	✓
Detailed descriptions of any instance of whistleblower retaliation	✓	✓	✓	✓

Source: GAO analysis of DIA, NGA, and NSA OIG semiannual reports from October 1, 2016, through September 30, 2018; NRO OIG semiannual reports from October 1, 2016, through March 31, 2018; and Title 5, Appendix, U.S. Code. | GAO-20-699

[40]In addition to reporting on investigative activities, both Title 5, Appendix, and Title 50, U.S. Code, require IC-element OIGs to report broadly on OIG activities, such as descriptions of significant problems, abuses, and deficiencies relating to the administration of programs and operations in the agencies, descriptions of the recommendations for corrective action made by the OIGs, and statistical tables showing the total number of reports and the total dollar value of questioned costs identified in those reports.

Semiannual reporting requirements for the ICIG and CIA OIG are codified in sections 3033 and 3517, respectively, of Title 50 of the United States Code. Sections 3033 and 3517 of Title 50 require that the ICIG and CIA OIG report, at a minimum, on the title or subject of investigations conducted during the reporting period, but these sections do not require the same level of detailed information for investigations as is required for the defense IC-element OIGs in section 5, Title 5, Appendix, United States Code. We reviewed the CIA OIG's semiannual reports covering the period from October 1, 2014, through March 31, 2018, and the ICIG's semiannual reports covering the period October 1, 2014, through September 30, 2019.[41] Table 3 provides a summary of Title 50 semiannual reporting requirements and the information provided by the ICIG and CIA OIG to meet those requirements.

Table 3: Intelligence Community Inspector General and Central Intelligence Agency Inspector General Compliance with Selected Statutory Requirements for Semiannual Reports

	Title 50 Reporting Requirements	Information Provided in Semiannual Reports
Inspector General of the Central Intelligence Agency (CIA OIG)	A list of the title or subject of each inspection, investigation, review, or audit conducted during the reporting period.[a]	The reports from the CIA OIG include general information about its Investigations Division, statistics about the total number and type of investigations conducted, and summaries of selected investigations completed in each reporting period.
Inspector General of the Intelligence Community (ICIG)	A list of the title or subject of each investigation, inspection, audit, or review conducted during the period covered by such report.[b]	Seven of the eight reports from the ICIG we reviewed included only general information about its Investigations Division and summaries of selected investigations completed in each reporting period. The most recent report—for the period covering April 1, 2019, through September 30, 2019—also added statistics about the total number and type of investigations conducted.

Source: GAO analysis of CIA OIG semiannual reports from October 1, 2014, through March 31, 2018; ICIG semiannual reports from October 1, 2014, through September 30, 2019; and 50 U.S.C. § 3033 and § 3517. | GAO-20-699

[a]50 U.S.C. § 3517

[b]50 U.S.C. § 3033

We found that the CIA OIG met its semiannual reporting requirements by providing statistical tables of all closed cases, broken out by type of investigation. Additionally, the CIA OIG provides summaries of selected investigations completed during the time frame of each semiannual report. According to CIA OIG officials, they do not provide a list of the

[41]We also reviewed semiannual reports for fiscal year 2019 from the ICIG because of additional information ICIG officials told us they included in those reports.

titles of investigations in the semiannual report in order to protect the integrity of the investigations, but the categories listed in the statistical tables provide information on the type of allegations involved in each investigation conducted in a given reporting period. For seven of the eight semiannual reports included in our scope from the ICIG that we reviewed, they provided summaries only of selected completed investigations, and did not provide a list of the titles or subjects of all investigations nor include statistical tables indicating the category of each investigation conducted in the applicable reporting period that would satisfy the statutory requirement. ICIG officials stated that they used reporting conventions established under prior leadership, and they could not comment on why this information was not provided in the past. However, the most recent report—for the period covering April 1, 2019, through September 30, 2019—includes statistics about the total number and types of investigations conducted, which meets the ICIG's semiannual reporting requirement.

Four IC-Element OIGs Have Reached an Agreement with the DOD OIG That Addresses Notification and Oversight Requirements

Several DOD policies establish requirements for the DOD OIG to provide oversight of all DOD-component OIG investigations—including those conducted by the DIA OIG, NGA OIG, NRO OIG, and NSA OIG, as well as those conducted by non-IC DOD components—and for DOD component OIGs to notify the DOD OIG of certain allegations and at specific points throughout their cases. For example, DOD Directive 5505.06*, Investigations of Allegations against Senior DOD Officials*, requires the DIA OIG, NGA OIG, NRO OIG, and NSA OIG to notify the DOD OIG within 5 days of receiving credible allegations of misconduct involving DOD senior officials. As noted above, we have previously reported that the DOD OIG and the defense IC-element OIGs had not fully addressed all oversight requirements. In 2017, we recommended that the DOD OIG work in coordination with the Secretary of Defense, the Under Secretary of Defense for Intelligence, and the defense IC-element OIGs to establish a process to fully implement oversight requirements.[42]

The DOD OIG, DIA OIG, NGA OIG, NRO OIG, and NSA OIG agreed to a memorandum of understanding in July 2019 that codified their existing practice of notifying the DOD OIG when an allegation is determined to be

[42]GAO-17-506. The DOD OIG concurred with and implemented this recommendation by completing the memorandum of understanding.

credible.[43] The memorandum is intended to clarify aspects of the relationship between the DOD OIG and the defense intelligence OIGs, enhance execution of their respective missions, and strengthen cooperation and collaboration among the DOD OIG and the defense intelligence OIGs. The memorandum states that defense intelligence OIGs are to notify the DOD OIG within 5 working days of receipt of any non-frivolous allegation of misconduct in which the subject of the allegation is a senior official, and to provide a copy of the complaint to the DOD OIG.[44] The memorandum also recognizes that the nature of the defense intelligence OIGs and operational and practical realities may necessitate accommodations from DOD guidance, and it establishes a mechanism to provide such accommodations.

In addition to the memorandum, DOD OIG officials stated that they are revising DOD Directive 7050.06, *Military Whistleblower Protection* (Apr. 17, 2015), governing military reprisal investigations across DOD to include longer time frames for components to determine whether an investigation is warranted and provide certain notifications to the DOD OIG. These officials said that similar revisions are likely needed for DOD's expired policy that governs the DIA OIG, NGA OIG, NRO OIG, and NSA OIG whistleblower reprisal investigations involving DOD civilian

[43]The DOD IG, DIA IG, NRO IG, NGA IG, and NSA IG, Secretary of Defense, and heads of the defense intelligence agencies were directed to establish this memorandum of understanding by the Senate Armed Services Committee in 2014. See S. Rep. No. 113-176 at 235-6 (2014) and GAO-17-506. In our review of IC-element OIG case files, we found that the IC-element OIGs provided notifications to the DOD OIG consistent with the memorandum of understanding, though not all cases required notification. For example, NRO OIG officials stated that during the period under review, they provided notification to the DOD OIG of one case involving alleged misconduct by a DOD senior official. No other NRO OIG cases in our review required notification to the DOD OIG because they did not involve DOD personnel.

[44]DOD Directive 5505.06 defines "senior official" as an active duty, retired, Reserve, or National Guard military officer in grades O-7 and above, and an officer selected for promotion to O-7 whose name is on the O-7 promotion board report forwarded to the Military Department Secretary; a current or former member of the Senior Executive Service; a current or former DOD civilian employee whose position is deemed equivalent to that of a member of the Senior Executive Service (e.g., Defense Intelligence Senior Executive Service, Senior Level employee, and non-appropriated fund senior executive); or a current or former Presidential appointee.

personnel.[45] DOD OIG officials stated in May 2019 that they were waiting for the Office of the Undersecretary of Defense for Intelligence to initiate efforts to revise that policy. A senior official from that office told us in July 2019 that the office had incorporated the whistleblower protections into a draft DOD instruction that governs the Defense Civilian Intelligence Personnel System. At that time, the official stated that this instruction was in internal coordination within DOD and was expected to be finalized by the end of December 2019. The official added that the draft Instruction would be coordinated with the Office of the Director of National Intelligence and the heads of DOD IC elements as part of the formal coordination process.

Three of the Selected IC-Element OIGs Did Not Consistently Document Notifications to Complainants in Reprisal Investigations We Reviewed

Two of the IC-element OIGs we reviewed, the CIA OIG and NSA OIG, provide formal notifications to complainants of the conclusion of their whistleblower reprisal investigations, informing them of their right to request an External Review Panel and providing contact information to make such a request.[46] Specifically, the CIA OIG requires that these memorandums be provided to the complainant and included in the case file. The CIA OIG closed two investigations in which this requirement applied during the time frame of our case file review—October 1, 2016, through March 31, 2018—and our review of their case files showed that it provided the memorandums, including the requisite information on External Review Panels, in both cases. The NSA OIG's procedures state that investigators should provide to the complainant a written, unclassified summary of investigative findings and a memorandum with instructions

[45]Directive-Type Memorandum 13-008. Although Directive-Type Memorandum 13-008 expired on Jan. 8, 2018, DOD OIG officials stated that they expect component OIGs to operate in accordance with its requirements until new whistleblower protection policies and procedures are finalized. DOD OIG officials stated that they have not communicated this general expectation to the DIA OIG, NGA OIG, NRO OIG, and NSA OIG.

[46]Office of the Director of National Intelligence policy requires the ICIG to formally notify complainants in whistleblower reprisal investigations of the results of the investigations and their rights to request an appeal via an External Review Panel. The ICIG was unable to identify any closed whistleblower reprisal investigations from October 1, 2016, through March 31, 2018, and, therefore, we were unable to confirm that this policy is followed in our case file review.

for requesting an External Review Panel.[47] The NSA OIG closed three unsubstantiated reprisal investigations between October 2016 and April 2018. Our review of their case files showed that the NSA OIG provided memorandums—including the requisite information requesting an External Review Panel or other review—in all cases.[48]

Officials from the three other IC-element OIGs for which we reviewed case files—the DIA OIG, NGA OIG, and NRO OIG—stated that notifications to complainants in reprisal investigations are normally provided informally, via phone or email. However, in our review of investigative case files, described below, we found that these informal notifications were not consistently documented.

- **DIA OIG:** We reviewed four reprisal cases at the DIA OIG that had unsubstantiated allegations and found memorandums to the complainants in three of them. In two of those three cases, the complainant was a defense civilian intelligence employee who was informed of the right to request an External Review Panel. In the other case, the complainant was a military servicemember who received information on applying for review by the Board for Correction of Military Records. The file for the fourth case we reviewed did not contain a memorandum to the complainant. The complainant in this case was a defense civilian intelligence employee, but the case file did not include evidence—such as investigator log entries or copies of email or memorandums—indicating that the complainant was notified of the completion of the investigation or informed of the right to request an External Review Panel.

[47]The NSA OIG revised its investigations procedures in January 2019. The revised procedures incorporate an additional requirement that investigators provide complainants in unsubstantiated reprisal cases an opportunity to review the analysis and tentative conclusions before the report of investigation becomes final. This allows the complainants in these cases to clarify or provide additional information, and according to NSA OIG officials it facilitates the complainant's full understanding of the NSA OIG's rationale for its conclusions and increases their confidence in the system. However, because we reviewed only cases completed prior to March 30, 2018, this requirement did not apply to any of the cases that we reviewed.

[48]The complainants in two of the unsubstantiated reprisal investigations closed by the NSA OIG were civilian intelligence personnel covered by Presidential Policy Directive-19. The complainant in the third case was an active duty Navy servicemember. Section 1034(g) of Title 10, United States Code, provides servicemembers with an appeal by requesting a review by their respective board for the correction of military records. In the case we reviewed, the NSA OIG informed the complainant of the complainant's right to request a review by the Board for Correction of Naval Records.

- **NGA OIG:** We reviewed three unsubstantiated reprisal cases at the NGA OIG. Although the investigators' logs for all three cases indicated that the complainants were contacted near the ends of the investigations, the log entries did not indicate whether the complainants were informed of their rights to request an External Review Panel or provided instructions for requesting a copy of the respective reports. Copies of the communications were not present in the official hard-copy case files we reviewed, but NGA OIG officials were able to identify a memorandum in their electronic case management system with information on the complainant's right to request an External Review Panel for one of the cases. NGA OIG officials explained that there was a period of time during which they did not provide formal notifications to the complainant, but information was typically provided to a complainant either via an informal email or telephone call. The officials also stated that they may transition to using fully electronic case files in the future, which we believe could help mitigate this issue.
- **NRO OIG:** We reviewed two unsubstantiated reprisal cases at the NRO OIG. The complainant in each case was a contractor. The OIG notified one complainant via email that it had closed the investigation—documentation of which we saw in our review of the case file. The second complainant was notified of the completion of the OIG's investigation via telephone by the OIG, according to NRO OIG officials. Documentation of the phone call was not present in the case file at the time of our review, but was subsequently provided by the NRO OIG. At the time of the respective investigations, contractors did not have the right to request an External Review Panel, and as discussed below, NRO OIG procedures did not require retention of complainant correspondence in the case files.

All IC-element OIGs we reviewed have policies or investigation procedures that require them to provide information to complainants about the results of any investigations into allegations of whistleblower reprisals made by them. Additionally, four OIGs—the CIA OIG, DIA OIG, ICIG, and NSA OIG—have policies that require them to formally notify complainants of their right to request an External Review Panel in unsubstantiated cases. Table 4 below summarizes the requirements in each IC element's policies or the IC-element OIG's procedures pertaining to communications with complainants who have made allegations of reprisals.

Table 4: Selected Intelligence Community (IC)-Element Policies and Office of Inspector General (OIG) Procedures for Communications to Whistleblowers in Reprisal Investigations

IC-element OIG	Description of policies and procedures
Central Intelligence Agency (CIA)	CIA's agency regulation on whistleblower protection assigns the CIA OIG responsibility for notifying the complainant in a reprisal investigation of the nature of the investigative findings and reason for any decision made prior to the conclusion of the investigation.[a] The regulation also sets forth CIA's policy that if the complainant disagrees with the findings of an OIG review or with CIA's decision regarding corrective actions, he or she may within 60 days request an external review panel from the ICIG as set forth in Presidential Policy Directive-19 and Intelligence Community Directive 120.
Defense Intelligence Agency (DIA)	DIA's instruction for whistleblower protection states that the DIA OIG shall upon completion of the investigation provide the Director of DIA, management, and the complainant, if applicable, with results of reviews and investigations.[b] The DIA OIG's supplemental procedures for whistleblower reprisal cases state that investigators are to formally notify the complainant if his or her allegation does not meet the legal elements of a whistleblower reprisal within 15 business days, formally notify the complainant of the results of the full investigation via written correspondence within 10 business days after the publication of the report of investigation, and, if the reprisal allegation is not substantiated, to include in that notification appeal rights for the complainant.
Intelligence Community Inspector General (ICIG)	The Office of the Director of National Intelligence has a whistleblower protection policy that states that the ICIG is responsible for notifying a complainant who makes a whistleblower reprisal allegation in writing of a determination that the complaint does not support a reprisal allegation. The policy also states that when the ICIG conducts an investigation involving reprisal, the ICIG is responsible for notifying the complainant in writing of the investigation's findings with instructions on how to obtain a copy of the summary of investigation should the complainant choose to request a copy.[c] The policy also acknowledges an individual's right to request an external review panel review if the investigation does not substantiate the reprisal allegation.
National Geospatial-Intelligence Agency (NGA)	The NGA OIG's investigations procedures state that as part of the case closure process, complainants in whistleblower reprisal investigations should be notified whether their complaints were or were not substantiated. The procedures also include a notification memorandum template that includes language about the complainant's rights for an external review by the ICIG.
National Reconnaissance Office (NRO)	As of February 2019, the NRO OIG's draft investigations manual stated that when the facts of a whistleblower reprisal investigation do not support the allegation, the investigator will provide to the complainant timely notification of the investigation results, the complainant's right to appeal, and contact information for the ICIG, which may conduct an external review of the NRO OIG's finding as cited in Intelligence Community Directive 120.
National Security Agency (NSA)	NSA's whistleblower protection policy requires the NSA OIG to notify the complainant of the investigative findings after the issuance of the report of investigation and inform the complainant that, if he or she has exhausted the applicable review process required by Presidential Policy Directive-19, then he or she may request an external review by an External Review Panel.[d] Additionally, the NSA OIG's investigations procedures state that for reprisal cases, investigators should schedule a personal meeting with the complainant, provide a written unclassified summary of investigative findings to review and make comments before a final report is completed, and advise the complainant of his or her appeal rights in writing.

Source: GAO review of IC-element whistleblower protection policies and OIG investigation procedures. | GAO-20-699

[a]CIA Agency Regulation [number withheld], Protecting Whistleblowers with Access to Classified Information (December 12, 2017).

[b]DIA Instruction 7050.200, Whistleblower Protection (August 1, 2019).

[c]Office of the Director of National Intelligence Instruction 20.04, Whistleblower Protections and Review of Allegations of Reprisal against Whistleblowers (July 3, 2013).

[d]NSA/Central Security Service Policy 1-62, Whistleblower Protection (June 24, 2015).

Additionally, five of the six IC-element OIGs have investigation procedures that require investigators to document investigative activities, including correspondence, in the investigative case files. The sixth—NRO OIG—has language in its draft procedures as of February 2019 indicating that correspondence may be retained in the investigative case file. Table 5 provides a summary of IC-element OIG procedures for documenting correspondence related to an investigation.

Table 5: Selected Intelligence Community (IC)-Element Office of Inspector General (OIG) Procedures for Documenting Whistleblower Communications

IC-element OIG	Description of procedures
Central Intelligence Agency (CIA)	The CIA OIG's investigations procedures state that all official correspondence, internal and external, to include correspondence with the complainant, is to be recorded in the official case file. The CIA OIG's procedures also state that complainants in reprisal investigations are to be notified in writing within 15 days of the completion of the investigation.
Defense Intelligence Agency (DIA)	The DIA's procedures for investigations state that operational material about an investigation, including correspondence, should be retained in the appropriate electronic case file.
Intelligence Community Inspector General (ICIG)	The ICIG's investigations procedures state that the investigation files should include detailed, extensive case notes of all correspondence and, if used, copies of notification letters.
National Geospatial-Intelligence Agency (NGA)	The NGA OIG's investigations procedures state that the case file will include key investigation records for the investigation, including correspondence documents.
National Reconnaissance Office (NRO)	As of February 2019, the NRO OIG's draft investigations procedures stated that that the case folder may contain complainant correspondence, but the manual does not require retention of complainant correspondence.
National Security Agency (NSA)	The NSA OIG's investigations procedures state that investigators should contemporaneously record all investigative activity in the NSA OIG's electronic case management system, to include a brief description of the activity and the date of that activity. The procedures also state that the hardcopy case file should contain all memorandums for the record and correspondence related to the investigation.

Source: GAO review of IC-element OIG investigation procedures. | GAO-20-699

While the DIA OIG, NGA OIG, and NRO OIG have policies in place to notify complainants in whistleblower reprisal investigations of the investigation results and to document those correspondences, these investigative activities were not consistently documented in the files we reviewed. These three IC-element OIGs were not aware that this documentation was not in the case files until we brought it to their attention, and neither NGA OIG nor NRO OIG offered an explanation of why it was not present. DIA OIG officials told us that for this specific case, the investigator recorded in their daily activities log that a conversation with the complainant occurred about other issues, but the investigator failed to fully document that they also discussed a notification of investigative findings. Taking steps to ensure that notifications to

complainants are documented in investigative case files would provide the DIA OIG, NGA OIG, and NRO OIG with greater assurance that they consistently inform reprisal complainants of the status of their investigations and their rights as whistleblowers.

Conclusions

Whistleblowers in the IC play an important role in detecting fraud, waste, and abuse, and—given that their work often involves sensitive and classified information—they face unique challenges in coming forward with a complaint. IC-element OIG investigations are critical to help ensure that whistleblowers are not retaliated against and that their complaints are properly handled. The time frames of investigations in the IC can be affected by a number of factors, but the ICIG and NGA OIG could improve their ability to manage investigation time frames by establishing specific, measurable timeliness objectives for their investigations in their investigative policies and procedures. All six of the selected IC-element OIGs have implemented a number of quality assurance processes for their whistleblower investigations, however, each selected IC-element OIG would also benefit from additional or improved quality assurance processes. Each selected IC-element OIG has provided training to its investigators, and the investigators we interviewed all stated that managers are supportive of investigators' training requests. However, the NSA OIG, ICIG, and NRO OIG do not have documented training plans that systematically link the requisite knowledge, skills, and abilities and training requirements to an investigator's career progression. Doing so could better ensure that their investigators possess a consistent set of professional competencies throughout their entire career progression. Finally, the DIA OIG, NGA OIG, and NRO OIG could better ensure that complainants are fully informed on the status of their investigations and their rights as whistleblowers by documenting complainant notifications in investigative case files.

Recommendations for Executive Action

We are making a total of 23 recommendations, including six to the ICIG (recommendations 1-6), three to the CIA OIG (recommendations 7-9), three to the DIA OIG (recommendations 10-12), three to the NGA OIG (recommendations 13-15), six to the NRO OIG (recommendations 16-21), and two to the NSA OIG (recommendations 22-23).

- The Inspector General of the IC should establish specific timeliness objectives for completing investigations conducted by the OIG of the IC. (Recommendation 1)

- The Inspector General of the IC should establish a time frame to finalize revisions to the OIG's investigations manual. (Recommendation 2)
- The Inspector General of the IC should establish a process to regularly review and update the OIG's investigative procedures. (Recommendation 3)
- The Inspector General of the IC should develop and implement a quality assurance program for the OIG's investigations division. This program should consist of routine internal and external quality assurance reviews consistent with CIGIE standards and guidance. (Recommendation 4)
- The Inspector General of the IC should develop a process to facilitate external quality assurance reviews of other IC-element OIGs' investigations divisions. (Recommendation 5)
- The Inspector General of the IC should ensure that as the ICIG finalizes its draft investigations procedures and investigator training plan, these documents provide an approach that systematically links the requisite knowledge, skills, and abilities and training requirements throughout an investigator's career progression. (Recommendation 6)
- The Inspector General of CIA should establish a time frame to finalize revisions to the OIG's investigations manual. (Recommendation 7)
- The Inspector General of CIA should establish a process to regularly review and update the OIG's investigative manual and policies. (Recommendation 8)
- The Inspector General of CIA should implement routine internal quality assurance reviews as part of the quality assurance program for the OIG's investigations divisions consistent with CIGIE standards and guidance. (Recommendation 9)
- The Inspector General of DIA should establish a process to regularly review and update the OIG's investigative procedures. (Recommendation 10)
- The Inspector General of DIA should implement routine external quality assurance reviews in the quality assurance program for the OIG's investigations division consistent with CIGIE standards. (Recommendation 11)
- The Inspector General of DIA should take steps to ensure that notifications to complainants in reprisal cases occur and are documented in the investigative case file, as required by OIG policy. (Recommendation 12)

- The Inspector General of NGA should establish specific timeliness objectives for completing investigations conducted by the OIG of NGA. (Recommendation 13)
- The Inspector General of NGA should develop and implement a quality assurance program for the OIG's investigations division. This program should consist of routine internal and external quality assurance reviews consistent with CIGIE standards and guidance. (Recommendation 14)
- The Inspector General of NGA should take steps to ensure that notifications to complainants in reprisal cases occur and are documented in the investigative case file, as required by OIG policy. (Recommendation 15)
- The Inspector General of NRO should establish a time frame to finalize the OIG's draft investigations manual. (Recommendation 16)
- The Inspector General of NRO should establish a process to regularly review and update the OIG's investigative procedures. (Recommendation 17)
- The Inspector General of NRO should continue to develop and implement a quality assurance program for the OIG's investigations division, which should incorporate routine internal and external quality assurance reviews consistent with CIGIE standards and guidance. (Recommendation 18)
- The Inspector General of NRO should consider making the use of documented investigative plans a requirement for all investigations. (Recommendation 19)
- The Inspector General of NRO should revise its training plan to provide an approach that systematically links the requisite knowledge, skills, and abilities to training requirements throughout an investigator's career progression. (Recommendation 20)
- The Inspector General of NRO should take steps to ensure that notifications to complainants in reprisal cases occur and are documented in the investigative case files, as required by OIG policy. (Recommendation 21)
- The Inspector General of NSA should develop and implement a quality assurance program for the OIG's investigations division. This program should consist of routine internal and external quality assurance reviews consistent with CIGIE standards and guidance. (Recommendation 22)

- The Inspector General of NSA should develop an investigator training plan that provides an approach that systematically links the requisite knowledge, skills, and abilities to training requirements to an investigator's career progression. (Recommendation 23)

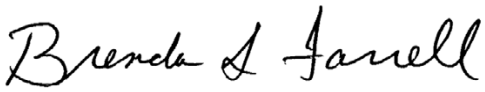
Agency Comments and Our Evaluation

We provided a draft of the sensitive report to the Inspectors General of the IC, CIA, DIA, NGA, NRO, NSA, and DOD for review and comment. In their responses on the sensitive report, reproduced in appendixes IV-X respectively, the IC-element OIGs and the DOD OIG concurred with all of our recommendations.

The ICIG, CIA OIG, DIA OIG, NSA OIG, and NRO OIG also provided technical comments on the sensitive report, which we incorporated as appropriate.

We are sending copies of this report to the appropriate congressional committees, the Secretary of Defense, the Director of National Intelligence, and the Inspectors General of the IC, CIA, DIA, NGA, NRO, NSA, and DOD, and other interested parties. In addition, the report is available at no charge on the GAO website at https://www.gao.gov.

If you or members of your staff have any questions regarding this report, please contact Brenda S. Farrell at (202) 512-3604 or farrellb@gao.gov, or Brian M. Mazanec at (202) 512-5130 or mazanecb@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this report are listed in appendix XI.



Brenda S. Farrell
Director
Defense Capabilities and Management

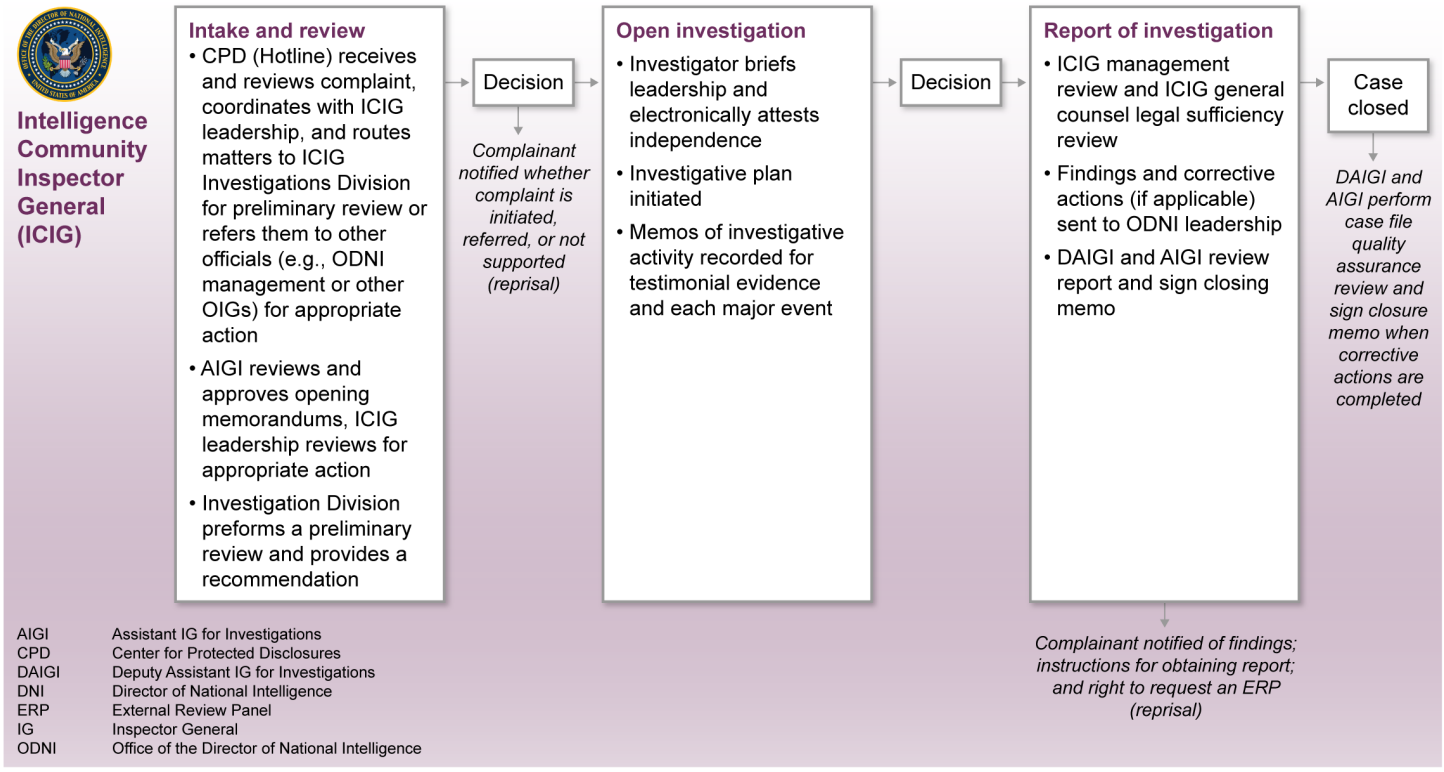
Brian M. Mazanec
Director
Defense Capabilities and Management

Appendix I: Intelligence Community (IC)-Element Offices of Inspector General's (OIG) Hotline and Investigative Processes

IC-element OIGs have processes for receiving, vetting, and investigating complaints. Each IC-element OIG operates a hotline program that is responsible for receiving complaints; determining the credibility of the information initially provided by complainants; creating a record of the complaint in the OIG's case management system; and routing relevant information to the appropriate officials. Generally, upon receiving a complaint, hotline managers and supervisors may decide not to investigate a complaint if it lacks credibility or sufficient detail to conduct investigative work, or they may direct the complainant to IC-element management or to another OIG if the complaint involves matters that are outside the OIG's authority to investigate potential fraud, waste, or abuse and potential violations of law, regulation, or policy. Hotline officials may also refer certain complaints to another entity if (1) there is no possibility of disclosing the identity of the complainant or (2) the complainant consents to the referral when there is a possibility of disclosing his or her identity.

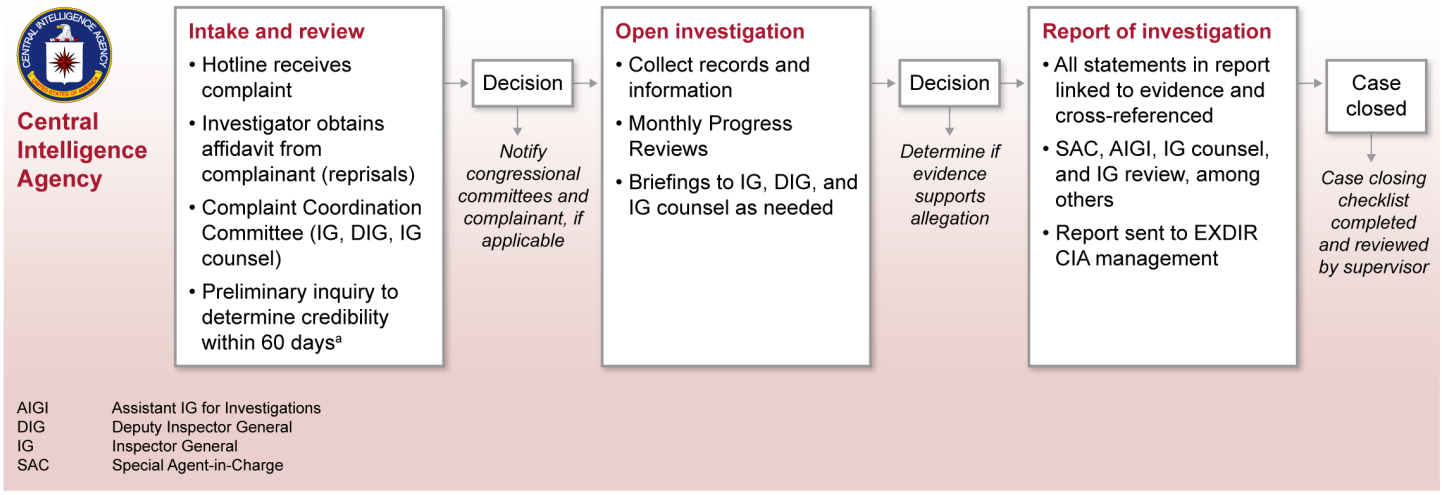
If hotline officials determine that a complaint is credible and within the purview of the OIG, they are typically to provide the complaint to the IC-element OIG's investigative managers and staff, who may further vet the complaint and determine whether to conduct a full investigation according to the respective OIG's processes and procedures. The figures below provide high-level representations of each IC-element OIG's respective processes for receiving, vetting, and investigating complaints.

Figure 3: Inspector General of the Intelligence Community (ICIG) Hotline and Investigative Process



Source: GAO analysis of Intelligence Community Inspector General information. | GAO-20-699

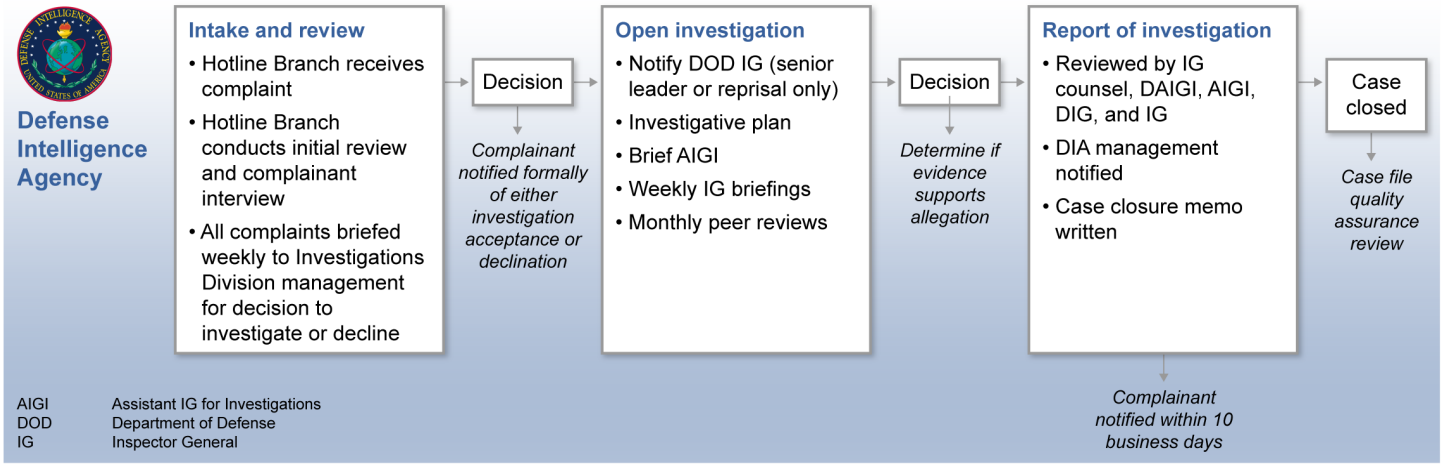
Figure 4: Central Intelligence Agency (CIA) Office of Inspector General (OIG) Hotline and Investigative Process



Source: GAO analysis of Central Intelligence Agency information. | GAO-20-699

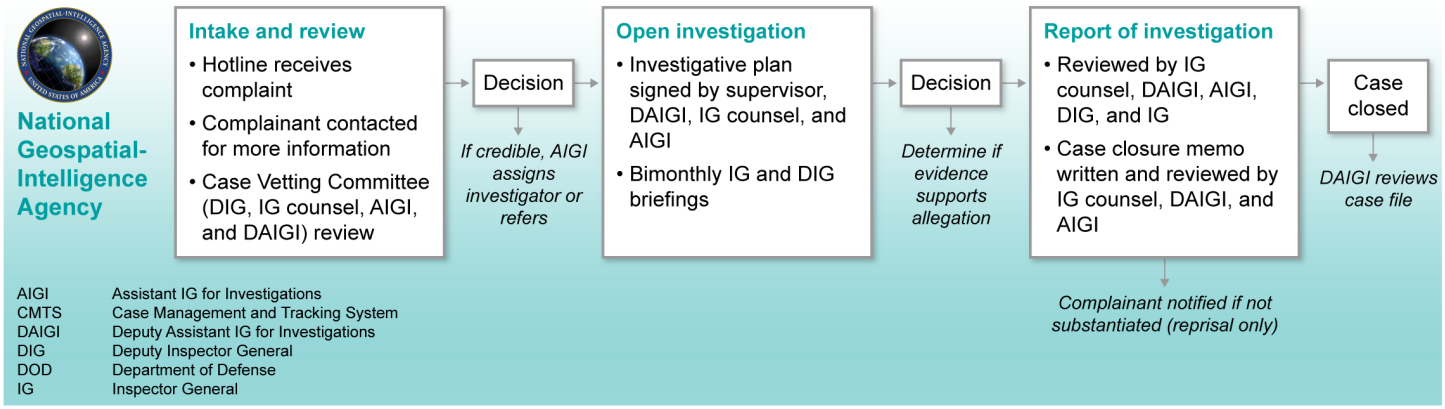
[a]The CIA OIG's procedures allow 60 days of preliminary investigative work for all complaints, which may be extended to 120 days with the approval of OIG management.

Figure 5: Defense Intelligence Agency (DIA) Office of Inspector General (OIG) Hotline and Investigative Process



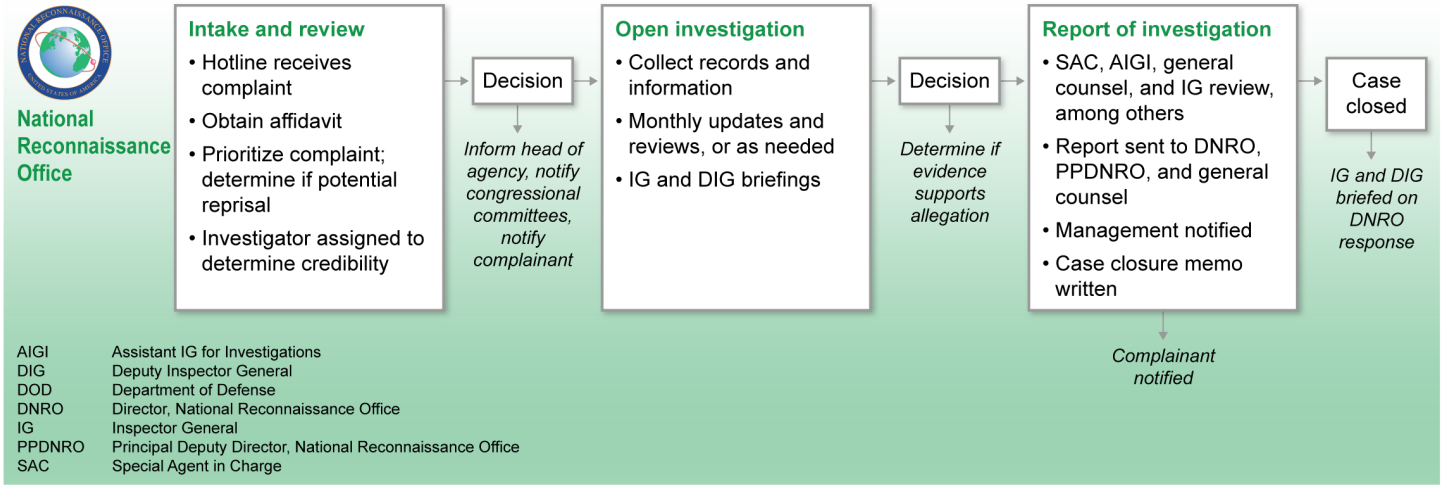
Source: GAO analysis of Defense Intelligence Agency information. | GAO-20-699

Figure 6: National Geospatial-Intelligence Agency (NGA) Office of Inspector General (OIG) Hotline and Investigative Process



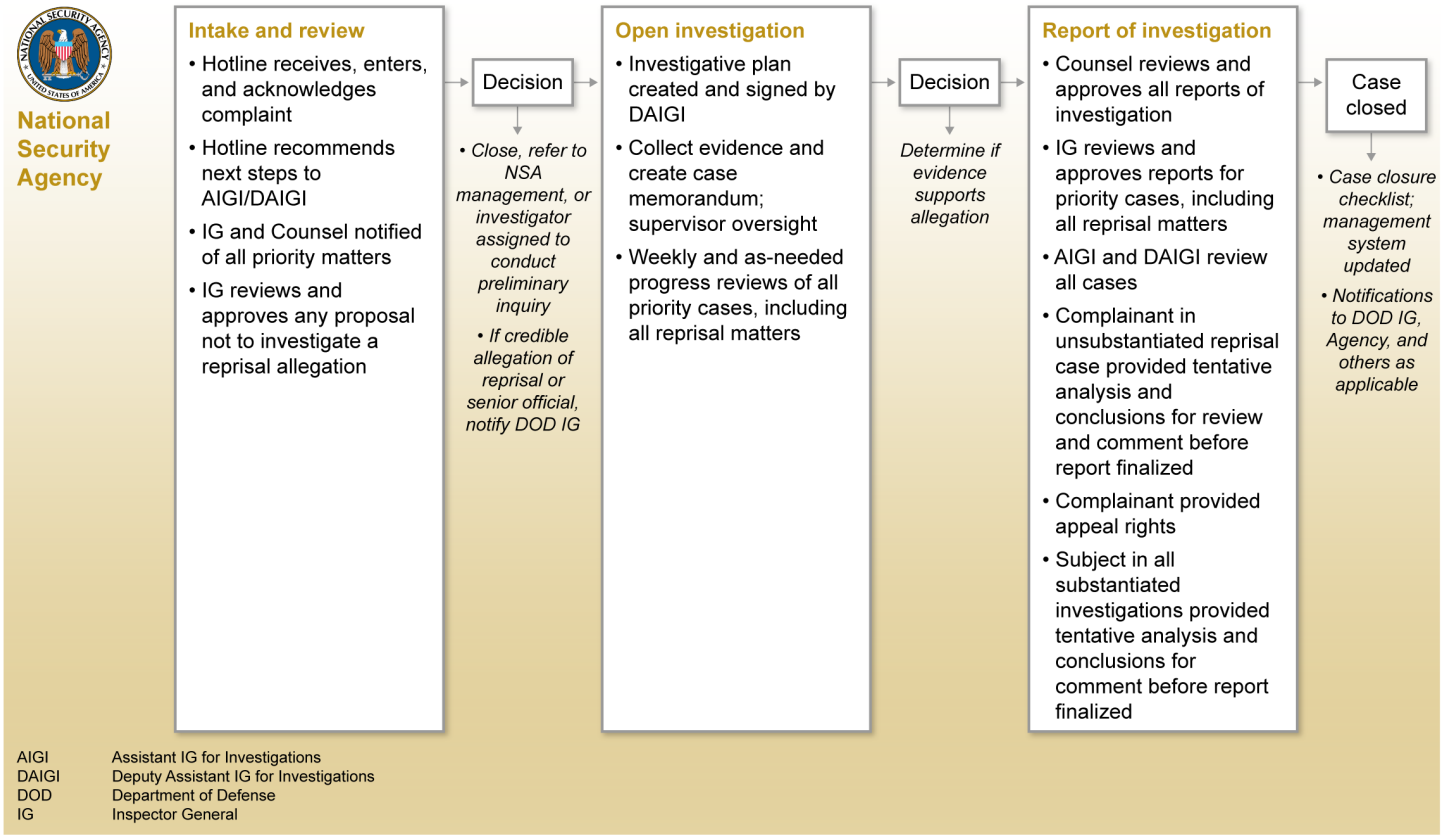
Source: GAO analysis of National Geospatial-Intelligence Agency information. | GAO-20-699

Figure 7: National Reconnaissance Office (NRO) Office of Inspector General (OIG) Hotline and Investigative Process



Source: GAO analysis of National Reconnaissance Office information. | GAO-20-699

Figure 8: National Security Agency (NSA) Office of Inspector General (OIG) Hotline and Investigative Process

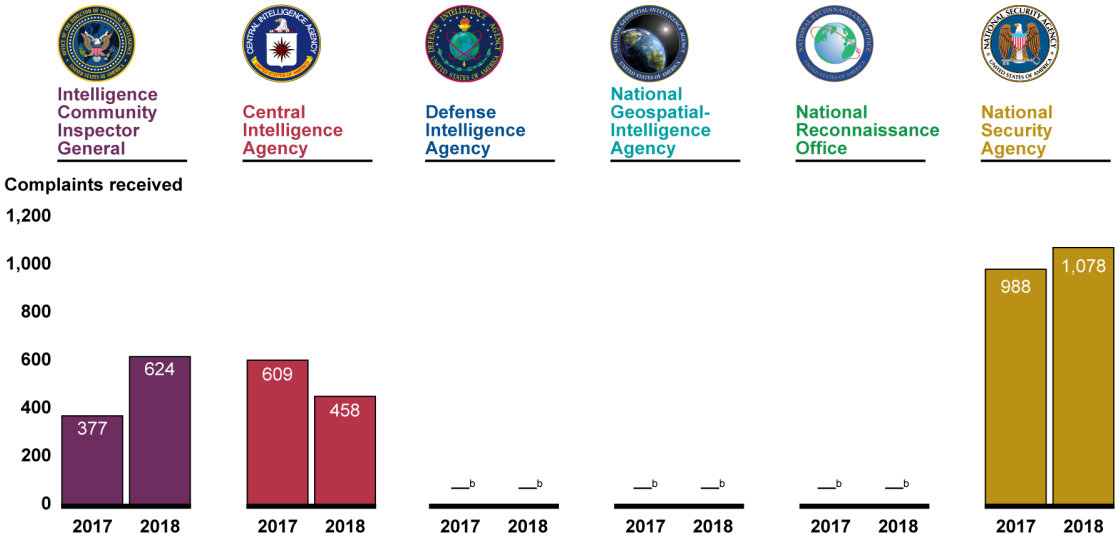


Source: GAO analysis of National Security Agency information. | GAO-20-699

Appendix II: Statistics for Selected Intelligence Community (IC)-Element Offices of Inspector General (OIG) Investigations

This appendix provides detailed information on the number of complaints received by each of the selected IC-element OIGs in fiscal years 2017 and 2018, as well as the distribution of investigation time frames, by IC-element OIG. The number of investigations at each of the IC-element OIGs varies widely, based on factors such as the number of complaints received by each IC-element OIG and the fact that each OIG makes its own determination on when to convert a complaint into an investigation. For example, CIA OIG procedures allow up to 120 days for preliminary investigative work to assess the credibility of a complaint, while DIA OIG procedures allow for only 10 days if the complaint involves activities in the continental United States.[1]

Figure 9: Complaints Received and Investigated by Intelligence Community (IC)-element Offices of Inspector General (OIG) in Fiscal Years 2017 and 2018



	Intelligence Community Inspector General		Central Intelligence Agency		Defense Intelligence Agency		National Geospatial-Intelligence Agency		National Reconnaissance Office		National Security Agency	
	2017	2018	2017	2018	2017	2018	2017	2018	2017	2018	2017	2018
Investigations opened	18	13	41	32	96	61	154	122	58	35	159	171
Ongoing investigations as of Aug. 2019[a]	2	2	—[b]	—[b]	2	10	3	12	7	8	9	4

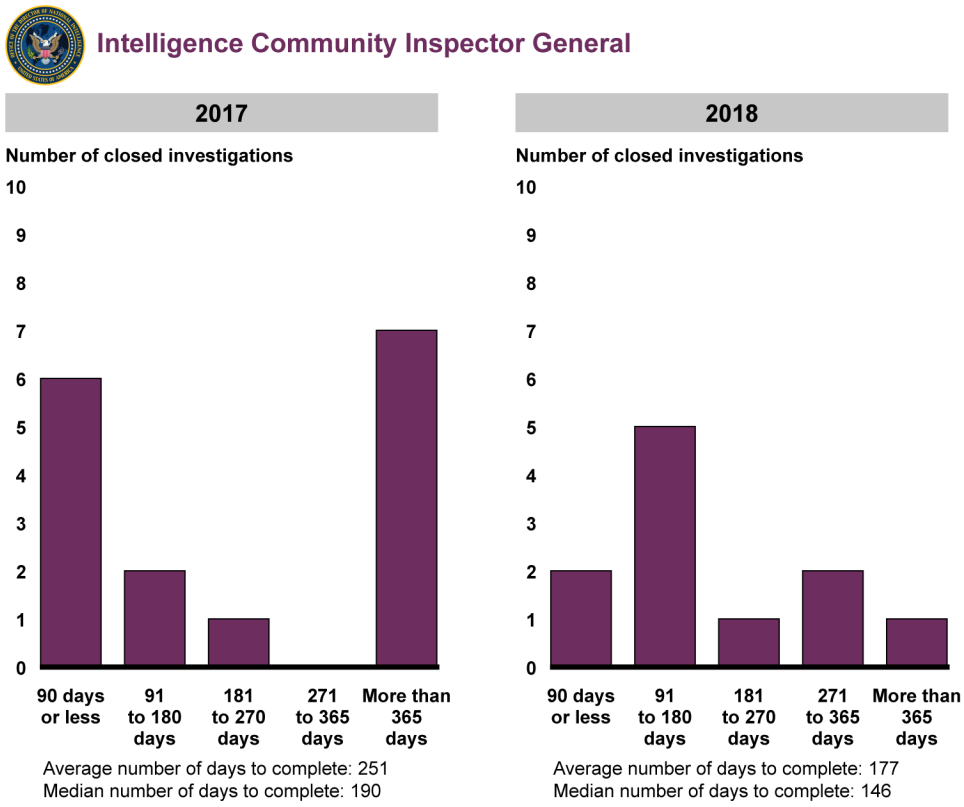
Source: GAO analysis of Intelligence Community-element data. | GAO-20-699

[a]Case times for open cases are calculated from the date each complaint was received through the following dates: ICIG (August 9, 2019); CIA OIG (August 6, 2019); DIA OIG (July 2, 2019); NGA OIG (July 1, 2019); NRO OIG (June 26, 2019); NSA OIG (June 28, 2019).

[b]Specific details of the investigation statistics for the CIA OIG, DIA OIG, NGA OIG, and NRO OIG were omitted because the IC elements deemed that the information is sensitive.

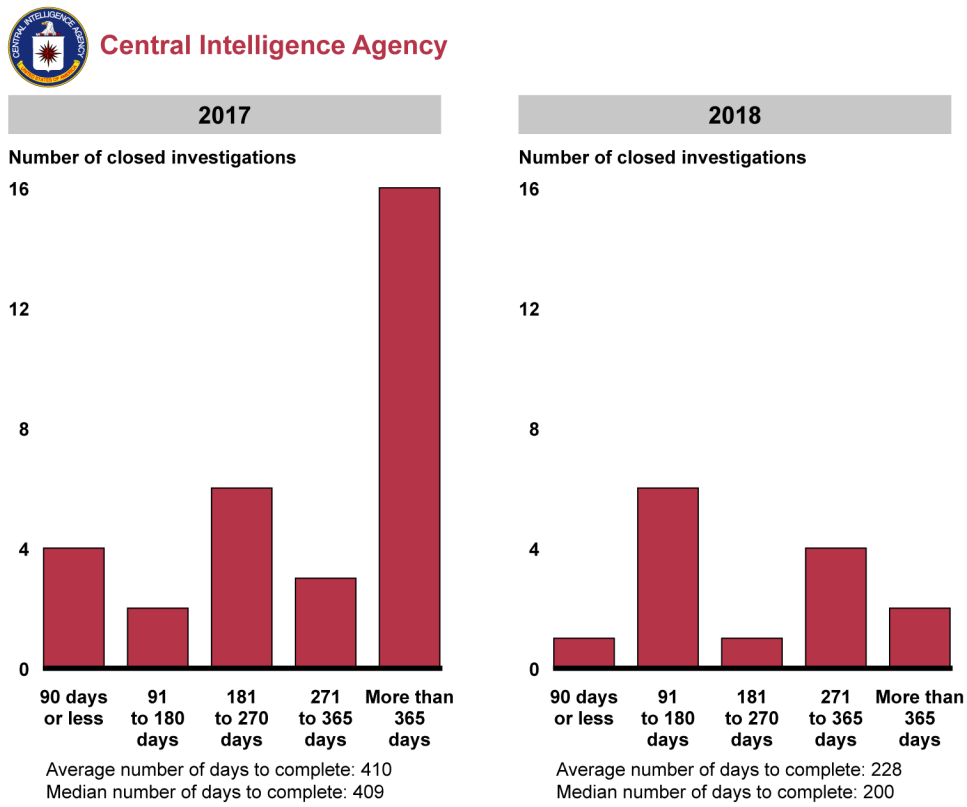
[1]Specifically, the CIA OIG's procedures allow 60 days of preliminary investigative work for all complaints, which may be extended to 120 days with approval of OIG management. The DIA OIG's procedures allow 30 days of preliminary investigative work for complaints that involve activities outside the continental United States.

Figure 10: Inspector General of the Intelligence Community (ICIG) Time Frames for Closed Investigations of Complaints Received in Fiscal Years 2017 and 2018



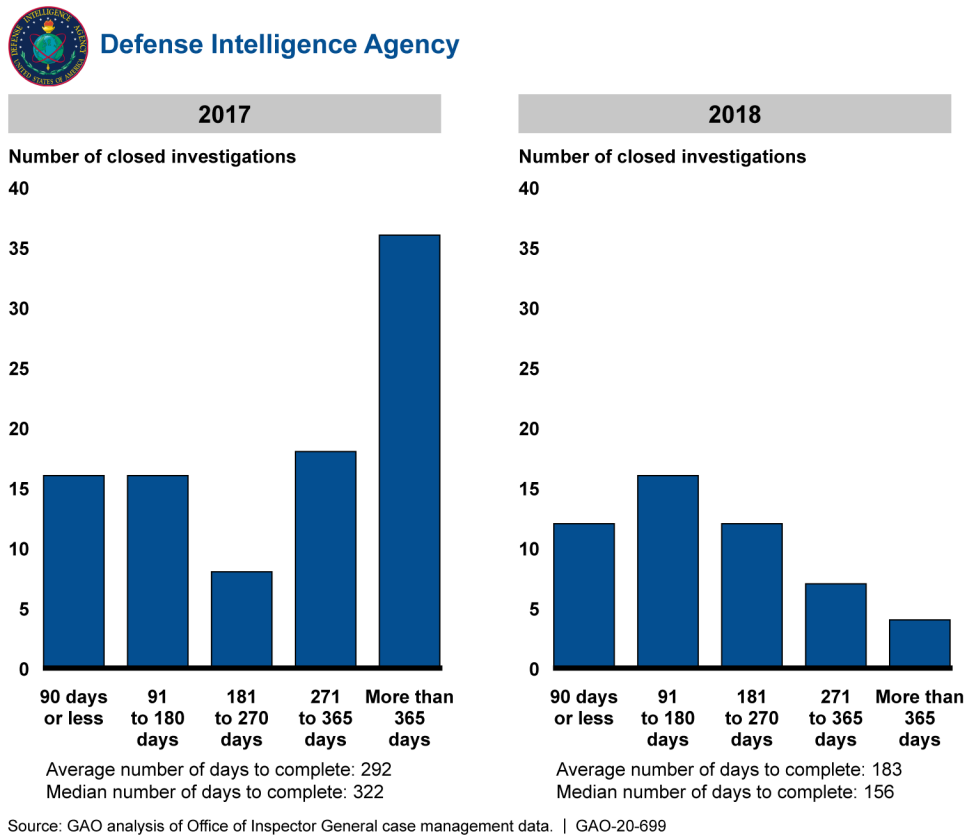
Source: GAO analysis of Office of Inspector General case management data. | GAO-20-699

Figure 11: Central Intelligence Agency (CIA) Office of Inspector General (OIG) Time Frames for Closed Investigations of Complaints Received in Fiscal Years 2017 and 2018



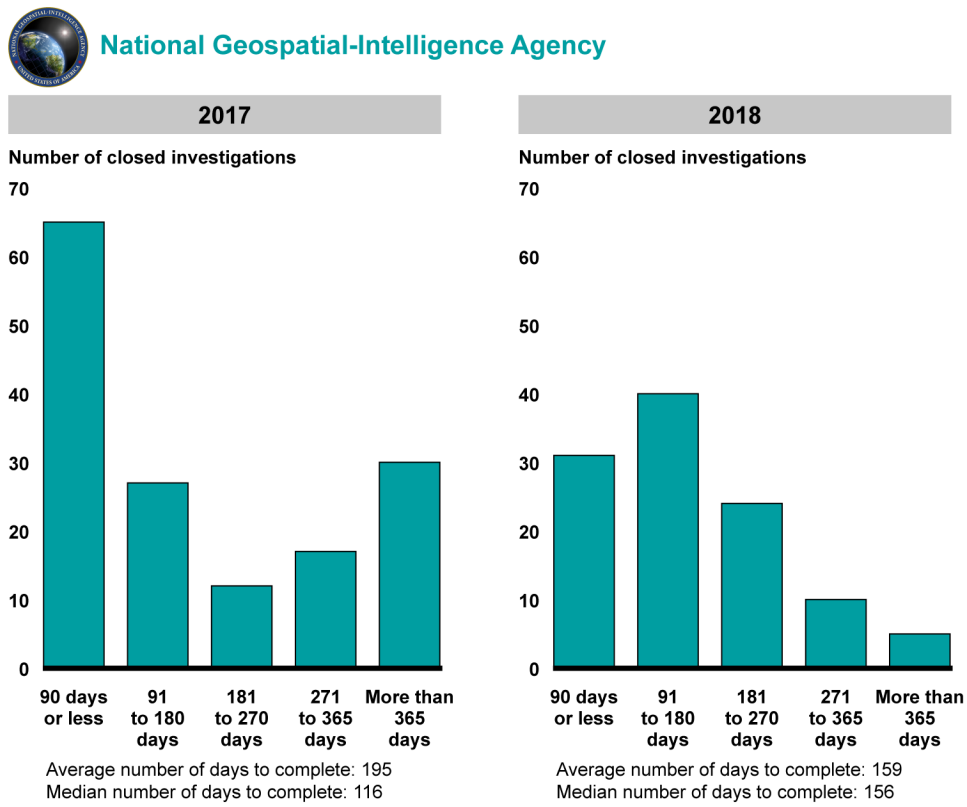
Source: GAO analysis of Office of Inspector General case management data. | GAO-20-699

Figure 12: Defense Intelligence Agency (DIA) Office of Inspector General (OIG) Time Frames for Closed Investigations of Complaints Received in Fiscal Years 2017 and 2018



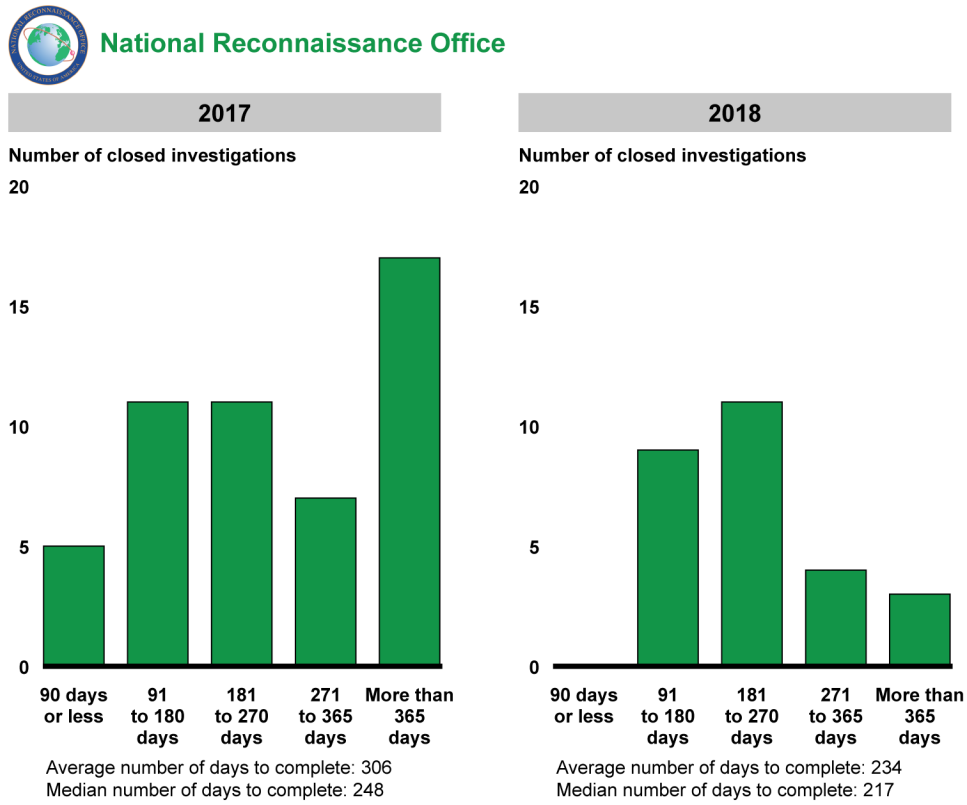
Source: GAO analysis of Office of Inspector General case management data. | GAO-20-699

Figure 13: National Geospatial-Intelligence Agency (NGA) Office of Inspector General (OIG) Time Frames for Closed Investigations of Complaints Received in Fiscal Years 2017 and 2018



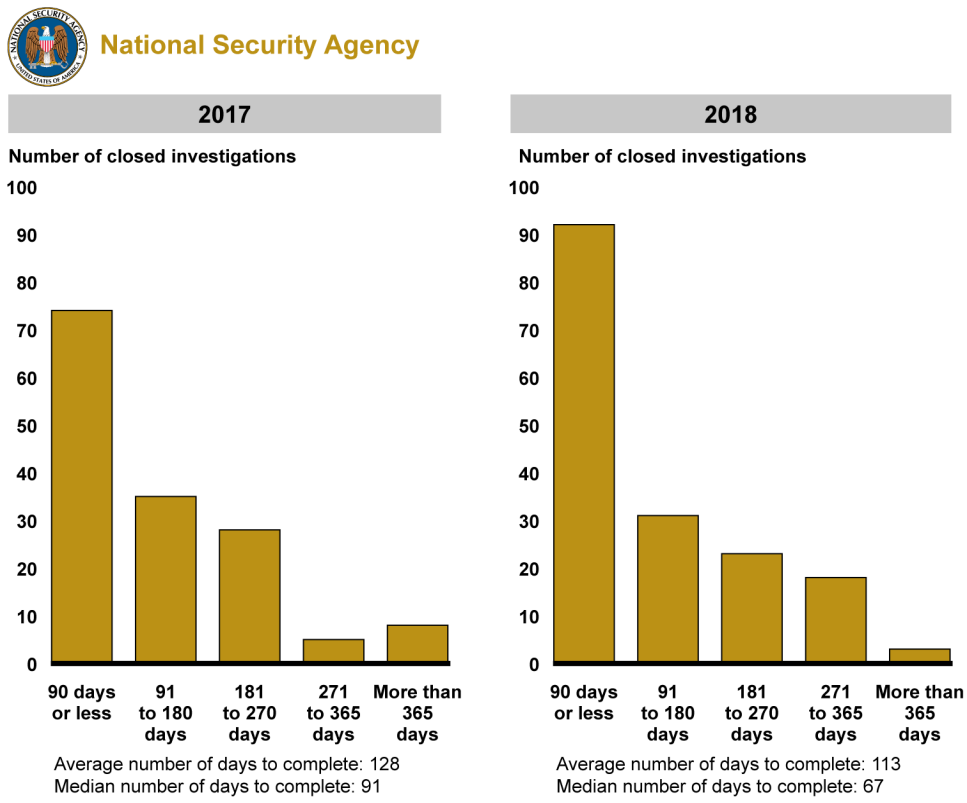
Source: GAO analysis of Office of Inspector General case management data. | GAO-20-699

Figure 14: National Reconnaissance Office (NRO) Office of Inspector General (OIG) Time Frames for Closed Investigations of Complaints Received in Fiscal Years 2017 and 2018



Source: GAO analysis of Office of Inspector General case management data. | GAO-20-699

Figure 15: National Security Agency (NSA) Office of Inspector General (OIG) Time Frames for Closed Investigations of Complaints Received in Fiscal Years 2017 and 2018



Source: GAO analysis of Office of Inspector General case management data. | GAO-20-699

Appendix III: List of Intelligence Community (IC) Whistleblower Protection Laws, Policies, and Quality Standards

Whistleblowers are protected from reprisal as a result of making a protected disclosure through various statutes, regulations, and presidential policy covering Intelligence Community (IC) employees, military servicemembers, and contractors. This appendix provides information on the statutes, presidential directive, and agency directives and regulations that establish or incorporate protections from reprisal across the IC. It also includes information on quality standards for the investigative operations of federal offices of inspectors general.

Statutes

Inspector General Act of 1978, Pub. L. No. 95–452, and codified as amended at Title 5, Appendix, U.S. Code.

Intelligence Community Whistleblower Protection Act of 1998, Pub. L. No. 105-272, §§ 701-702 (1998) codified as amended at 5 U.S.C. §8H, Appendix; 50 U.S.C. § 3033; and 50 U.S.C. § 3517.

Intelligence Authorization Act of 2010, Pub. L. No. 111-259 (2010), and codified as amended at 50 U.S.C. §§ 3033 and 3517.

Intelligence Authorization Act of 2014, Pub. L. No. 113-126 (2014), codified as amended at 50 U.S.C. § 3234.

Foreign Intelligence Surveillance Act Amendments Reauthorization Act of 2017, Pub. L. No. 115-118, § 110, (2018).

Damon Paul Nelson and Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020, Pub. L. No. 116-92 (2019).

10 U.S.C. § 1034.

Presidential Policy Directives

The White House, Presidential Policy Directive 19, *Protecting Whistleblowers with Access to Classified Information* (Oct. 10, 2012).

IC-Element and Federal Department Policies, Regulations, and Directives

Central Intelligence Agency Regulation *[number withheld], Employee and Contractor Communications with Congress* (April, 8 2009).

Central Intelligence Agency Regulation *[number withheld], Protecting Whistleblowers with Access to Classified Information* (December 12, 2017).

Defense Intelligence Agency Instruction 7050.002, *Whistleblower Protection* (June 24, 2013).

Department of Defense Directive-Type Memorandum 13-008, *DOD Implementation of Presidential Policy Directive 19* (July 8, 2013, incorporating change 3, February 9, 2016).[1]

Department of Defense Instruction 1400.25, volume 2001, *DOD Civilian Personnel Management System: Defense Civilian Intelligence Personnel System (DCIPS) Introduction* (Dec. 29, 2008, incorporating change 1, Mar. 17, 2014).[2]

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

Department of Defense Directive 5505.06, *Investigations of Allegations against Senior DOD Officials* (June 6, 2013).

National Geospatial-Intelligence Agency Instruction 1100.1, *Protecting Whistleblowers with Access to Classified Information* (July 29, 2014, administrative update November 4, 2015).

National Reconnaissance Office Directive 80-6, *Protecting Whistleblowers with Access to Classified Information* (June 20, 2013).

National Security Agency/Central Security Service Policy 1-62, *Whistleblower Protection* (June 24, 2015).

Office of the Director of National Intelligence, *Intelligence Community Directive 120, Intelligence Community Whistleblower Protection* (March 20, 2014 with technical amendment, April 29, 2016).[3]

[1]Directive-Type Memorandum 13-008 expired in January 2018.

[2]According to a senior official with the Office of the Undersecretary of Defense for Intelligence, whistleblower protections previously implemented by Directive-Type Memorandum 13-008 will be incorporated into a forthcoming revision to DOD Instruction 1400.25, volume 2001.

[3]Intelligence Community Directive 120 is issued by the Director of National Intelligence and provides policies for whistleblower protection across the IC.

Office of the Director of National Intelligence, Intelligence Community Directive 701, *Unauthorized Disclosures of Classified National Security Information* (December 22, 2017).

Office of the Director of National Intelligence Instruction 20.04, *Whistleblower Protections and Review of Allegations of Reprisal against Whistleblowers* (July 3, 2013).[4]

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

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

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

CIGIE, *Qualitative Assessment Review Guidelines for Investigative Operations of Federal Offices of Inspector General* (July 18, 2017).

[4]ODNI Instruction 20.04 provides policies for whistleblower protection within the Office of the Director of National Intelligence. It includes policies for reprisal investigations conducted by the Inspector General of the Intelligence Community and procedures for External Review Panels.

Appendix IV: Comments from the Inspector General of the Intelligence Community

UNCLASSIFIED

OFFICE OF THE INSPECTOR GENERAL OF THE INTELLIGENCE COMMUNITY
WASHINGTON, D.C. 20511

May 28, 2020

Ms. Brenda Farrell
Mr. Brian M. Mazanec
Director, Defense Capabilities Management
U.S. Government Accountability Office
441 G Street, N.W.
Washington, DC 20548

Dear Ms. Farrell and Mr. Mazanec:

Thank you for your letter soliciting the Office of the Inspector General of the Intelligence Community's (IC IG's) review and comment on the U.S. Government Accountability Office (GAO) draft report entitled "Whistleblower Protection: Actions Needed to Strengthen Selected Intelligence Community Office of Inspector General Programs" (GAO-20-201SU). We sincerely appreciate the opportunity to review and I have enclosed the IC IG's responses. We concur with the recommendations in the report, which will further strengthen the IC IG's whistleblower program. We also offer several suggested revisions and updates, which we believe will make the report more accurate.

The subject of this report is an important one. Whistleblower protection and the investigation of whistleblower complaints is a vital mission for Inspectors General. The IC IG is committed to fighting fraud, waste, corruption, mismanagement, and abuses of authority, and protecting the whistleblowers who report them. It is imperative that Intelligence Community personnel have an impartial, effective program where whistleblowers are confident that they will be treated fairly, be safe from reprisal, and know that Inspectors General will take appropriate action when wrongdoing is reported.

As requested in your April 1, 2020 cover letter accompanying the draft report, the IC IG worked with the Office of the Director of National Intelligence's Information Management Division (IMD) to coordinate a sensitivity review of the draft report. IMD engaged with the appropriate offices within the National Geospatial-Intelligence Agency, National Security Agency, National Reconnaissance Office, Defense Intelligence Agency, and the Central Intelligence Agency to provide a coordinated response to your request. The IC IG provided the results of this review to GAO on May 17, 2020. IMD's coordinated sensitivity review suggested only minimal redactions to the draft report to protect sensitive (For Official Use Only) Intelligence Community information that cannot be released to the public.

UNCLASSIFIED

UNCLASSIFIED

Ms. Farrell and Mr. Mazanec

We are thankful for the GAO's work on this matter, and the professionalism and collegiality of the GAO team throughout the review. I hope you and your staff remain healthy and safe during these difficult times. Please contact the IC IG Legislative Counsel, Ms. Melissa Wright, or me if you have any additional questions or comments.

Sincerely,

Thomas A. Monheim
Acting Inspector General
of the Intelligence Community

Enclosures: IC IG Comments on GAO Recommendations
IC IG Proposed Revisions and Updates
IC IG Pamphlets
IC IG INV Career Path for Investigator

2

UNCLASSIFIED

UNCLASSIFIED

GAO-20-201SU (Report Dated May 2020)

"WHISTLEBLOWER PROTECTION: ACTIONS NEED TO STRENGTHEN SELECTED INTELLIGENCE COMMUNITY OFFICES OF INSPECTOR GENERAL PROGRAMS"

INSPECTOR GENERAL OF THE INTELLIGENCE COMMUNITY COMMENTS ON GAO RECOMMENDATIONS

We are thankful for the GAO's work on this matter, and the professionalism and collegiality of the GAO team throughout the review. We concur with the recommendations in the report, which will further strengthen the IC IG's whistleblower program.

Recommendation 1: The Inspector General of the IC should establish specific timeliness objectives for completing investigations conducted by the Office of the Inspector General of the IC.

IC IG Response: Concur. As part of its investigations manual revision process, IC IG will establish and incorporate timeliness objectives for completing investigations. IC IG will tailor its timeliness goals in accordance with its mission and the matters it undertakes. For example, many investigations conducted by IC IG have specific timeliness requirements designated by statute, including 270 days to complete External Review Panels and 14 days to decide an urgent concern matter. *See* 50 U.S.C. § 3236(c)(3); 50 U.S.C. § 3033(k)(5). Other investigations may involve novel issues or other complexities requiring more resources and time to complete in a thorough and objective matter. This includes IC IG's most impactful investigations, which often produce subsequent law enforcement investigations and court proceedings that can take years to complete. As in the past, IC IG will continue to adhere to the principle set forth in CIGIE's Quality Standards for Investigations that investigations "must be completed in a timely, efficient, thorough, objective manner."

Moreover, IC IG believes a careful, tailored approach to establishing timeliness objectives is appropriate to address the concern that some days-based metrics can be artificial measures of performance. For example, according to the report, OIGs with 180-day goals complete only 36% of investigations in less than 180 days, while OIGs without a specific days-based goal complete 67% of their investigations within 180 days, suggesting that the 180-day completion metric does not appear to be associated with the completion of investigations in less than 180 days. There also is a concern that an insufficiently tailored days-based metric may incentivize investigators to focus on minor matters that can be completed quickly and discourage the investigation of more complex allegations. Thus, in establishing timeliness objectives in response to the report's recommendation, IC IG will take into account that investigations can be fluid and unpredictable.

Recommendation 2: The Inspector General of the IC should establish a time frame to finalize revisions to the OIG's investigations manual.

IC IG Response: Concur. The Acting Assistant Inspector General for Investigations (A/AIGI) already has established a goal of completing the revisions within the next 180 days. Due in part

UNCLASSIFIED

to the additional requirements added in the Intelligence Authorization Act (IAA), the ongoing pandemic, and the recent departure of the AIG for investigations, IC IG has been unable to complete the revisions as originally anticipated. Accordingly, IC IG modified its timeline for completing the revision and intends issue its revised investigations manual before the end of calendar year 2020.

Recommendation 3: The Inspector General of the IC should establish a process to regularly review and update the OIG's investigative procedures.

IC IG Response: Concur. As part of its investigations manual revision process, the IC IG will establish a process to regularly review and update OIG's investigative procedures.

Recommendation 4: The Inspector General of the IC should develop and implement a quality assurance program for the OIG's investigations division. This program should consist of routine internal and external quality reviews consistent with CIGIE standards and guidance.

IC IG Response: Concur. The IC IG Investigations Divisions is undergoing several changes and we concur with developing a peer review process when those changes are complete. As explained in our June 2019 response to GAO, we currently anticipate that "once the management team is able to fill its open vacancies, revise its Manual, and train both incoming and existing staff on the new or revised policies and procedures, the Investigations Division might be in an appropriate position to be peer reviewed."

Recommendation 5: The Inspector General of the IC should develop a process to facilitate external quality assurance reviews of the IC-element OIGs' investigations divisions.

IC IG Response: Concur. The IC IG agrees that, similar to the role that the IC IG's Audit and Inspections and Evaluations team undertakes in coordinating peer reviews for the IC OIGs, this would be a useful coordination role for the IC IG Investigations Division to also undertake. The IC IG currently plans to address this recommendation at a future IC IG Forum meeting.

Recommendation 6: The Inspector General of the IC should ensure that as the IC IG finalizes its draft investigation procedures and investigator training plan, these documents provide an approach that systematically links the requisite knowledge, skills, and abilities and training requirements throughout an investigator's career progression.

IC IG Response: Concur. Any investigator training plan should link knowledge, skills, and abilities and training requirements with career progress. The IC IG Investigations Division's "Career Path for Investigator" document already requires the following trainings for advancement: Association of Certified Fraud Examiners (ACFE) Certified Fraud Examiner (CFE) Exam Review and continuing education; Essentials of Inspector General Investigations (EIGI); and DoD Whistleblowing / Reprisal; and further recommends 12 additional training programs. The "Career Path for Investigator," previously attached with our June 2019 response, lists trainings, skills, certifications, professional knowledge, work experiences, and competencies required for advancement. IC IG will ensure that appropriate training and advancement information is included as part of the investigations manual revision process.

Appendix V: Comments from the Inspector General of the Central Intelligence Agency

UNCLASSIFIED

Central Intelligence Agency

Office of Inspector General
703-374-8051

Washington, D.C. 20505

APR 30 2020

Ms. Brenda S. Farrell
Director, Defense Capabilities and Management
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Ms. Farrell:

This is CIA Office of Inspector General (OIG) response to the GAO Draft Report (GAO-20-201SU), "Whistleblower Protection: Actions Needed to Strengthen Selected Intelligence Community Offices of Inspector General Programs," dated May 20, 2020 (GAO Code 102577).

Attached is CIA OIG's response to the subject report. My point of contact is Assistant Inspector General for Investigations, Patrick D. Craddock, who can be reached at patridc3@ucia.gov, and 703-374-8937.

Sincerely,

Christine Ruppert
Acting Deputy Inspector General and
Counsel

UNCLASSIFIED

UNCLASSIFIED

GAO DRAFT REPORT DATED MAY 20, 2020
GAO-20-201SU

"WHISTLEBLOWER PROTECTION:
ACTIONS NEEDED TO STRENGTHEN SELECTED INTELLIGENCE COMMUNITY OFFICES OF INSPECTOR GENERAL PROGRAMS"

INSPECTOR GENERAL, CENTRAL INTELLIGENCE AGENCY COMMENTS TO THE GAO RECOMMENDATIONS

RECOMMENDATION 1: The GAO recommends that the Inspector General of the Central Intelligence Agency (CIA) should establish a time frame to finalize revisions to the Office of Inspector General's (OIG) investigations manual.

CIA OIG RESPONSE: Concur. The Inspector General of CIA established a time frame of no later than September 30, 2020, to finalize revisions to the OIG's investigations manual.

RECOMMENDATION 2: The GAO recommends that the Inspector General of CIA should establish a time process to regularly review and update the OIG's investigative manual and policies.

CIA OIG RESPONSE: Concur. The Inspector General of CIA is currently developing a process that will require the Office of Investigations to regularly review and update the Investigations manual, polices, and regulations. The requirement will be memorialized in a new chapter within the Investigations manual and incorporated into the annual Investigative work plan.

RECOMMENDATION 3: The GAO recommends that the Inspector General of CIA should implement routine internal quality assurance reviews as part of the quality assurance program for the OIG's investigations division consistent with Counsel of Inspectors General on Integrity and Efficiency (CIGIE) standards and guidance.

CIA OIG RESPONSE: Concur. The Inspector General of CIA will formalize a process and policy for the conduct of internal quality assurance reviews on investigative cases. This policy will be consistent with CIGIE standards and guidance in relation to investigations. The requirement will be memorialized in a new chapter within the Investigations manual and incorporated into the annual Investigative work plan.

UNCLASSIFIED

Appendix VI: Comments from the Inspector General of the Defense Intelligence Agency

DEFENSE INTELLIGENCE AGENCY

WASHINGTON, D.C. 20340-5100

U-20-0068/OIG

April 29, 2020

Ms. Brenda Farrell
Mr. Brian M. Mazanec
Director, Defense Capabilities Management
U.S. Government Accountability Office
441 G. Street, N.W.
Washington, DC 20548

Dear Ms. Farrell and Mr. Mazanec:

Please accept the enclosed as the Defense Intelligence Agency (DIA) Office of Inspector General (OIG) response to the U.S. Government Accountability Office (GAO) Draft Report GAO-20-201SU, "Whistleblower Protection: Actions Needed to Strengthen Selected Intelligence Community Office of Inspector General Programs," dated May 2020. We concur with recommendations 10, 11, and 12.

Prior to your oversight review, my office had taken steps to implement business processes that address the recommendations. We have since updated our investigation policies and procedures, and more actively engaged our Hotline Program in reviewing reprisal complaints. As an example of these process improvements, we now send formal notification memos to complainants when initiating a case and prior to publishing a report. Each memo includes Freedom of Information Act request information and outlines who they may contact for an external review of our investigative findings. In addition, our office now has an Assistant Inspector General for Quality Assurance, Integration, and Engagement who reviews investigation processes and procedures and ensures they comply with OIG standards.

My office and I are firmly committed to encouraging employees and others to report fraud, waste, and abuse, and to protecting whistleblowers from reprisal. I periodically release bulletins to all Agency employees encouraging reporting and reaffirming our commitment to protect whistleblowers rights. We do not disclose complainants' identities without their consent - unless disclosure is unavoidable, as required by the Inspector General Act. If disclosure is required, the complainant is notified prior to disclosure. We also prepare reports that do not—to the fullest extent possible—reveal the identity of complainants or those who provide information to our investigations. Furthermore, when we substantiate allegations, to include allegations of whistleblower reprisal, the Agency is required to notify our office of disciplinary actions taken, or reasons why actions were not taken. Consequently, in accordance with Presidential Policy Directive 19 should we identify a remediation action, we inform the Agency for consideration and request an official response.

We appreciate the opportunity to respond. Your recommendations will help ensure we continue to conduct thorough and impactful investigations including those related to whistleblowers.

More information regarding our whistleblower actions may be found in our Semiannual Reports to Congress at www.oig.dia.mil and www.oversight.gov.

The point of contact for this response is Special Agent Teresa Moses, Assistant Inspector General for Investigations, available at Teresa.Moses@dodiis.mil and (202) 231–1042.

Sincerely,

Kristi M. Waschull

Kristi M. Waschull
Inspector General

Enclosure: a/s

GAO DRAFT REPORT DATED APRIL 1, 2020
GAO-20-201SU (GAO CODE 102577)

"WHISTLEBLOWER PROTECTION: ACTIONS NEED TO STRENGTHEN SELECTED INTELLIGENCE COMMUNITY OFFICES OF INSPECTOR GENERAL PROGRAMS"

DEFENSE INTELLIGENCE AGENCY COMMENTS TO THE GAO RECOMMENDATION

RECOMMENDATION 10: The Inspector General should establish a process to regularly review and update the OIG's investigative procedures.

DIA OIG Response: Concur. Investigative processes are frequently changing and are codified in an Investigative Reminder, distributed to staff for immediate implementation. The reminders are stored in a Division shared folder for future incorporation to the SOP. The OIG's Investigations Division SOP, to include investigative processes, will be reviewed annually and updated as needed; not to exceed 2 years.

RECOMMENDATION 11: The Inspector General should implement routine external quality assurance reviews in the quality assurance program for the OIG's investigations division consistent with CIGIE Standards.

DIA OIG Response: Concur. During FY18-FY20 the OIG Investigations Division was subjected to an internal quality assurance review of processes and procedures. The quality assurance reviews will be conducted every 3 years to coincide with CIGIE Standards for peer reviews. The peer review of the investigations division planned for later this year will be postponed until next year due to the coronavirus-19 pandemic.

RECOMMENDATION 12—The Inspector General should take steps to ensure that notifications to complainants in reprisal cases occur and are documented in the investigative case file, as required by OIG policy.

DIA OIG Response: Concur. The OIG Investigations Division engaged in additional training, increased supervisory emphasis, and established case publication processes and a case closure checklist to ensure all actions and taskers are completed.

Appendix VII: Comments from the Inspector General of the National Geospatial-Intelligence Agency

UNCLASSIFIED

NATIONAL GEOSPATIAL-INTELLIGENCE AGENCY
7500 GEOINT Drive
Springfield, Virginia 22150

U-099-20/OIG

APR 2 2 2020

Ms. Brenda Farrell and
Mr. Brian M. Mazanec
Director, Defense Capabilities Management
U.S. Government Accountability Office
441 G Street, N.W.
Washington, DC 20548

Dear Ms. Farrell and Mr. Mazanec:

Enclosed is the National Geospatial-Intelligence Agency (NGA) Office of Inspector General (OIG) response to the GAO Draft Report GAO-20-201SU, "*Whistleblower Protection: Actions Needed to Strengthen Selected Intelligence Community Office of Inspector General Programs*," May 2020.

My point of contact is Ms. Patricia Langford, who can be reached at Patricia.C.Langford@nga.mil, and (571) 557-7487.

Sincerely,

Cardell K. Richardson, Sr.
Inspector General

Enclosure as stated

cc:
Director, Office of Corporate Communications

UNCLASSIFIED

UNCLASSIFIED

GAO Draft Report Dated May 2020
GAO-20-201SU

"Whistleblower Protection: Actions Needed to Strengthen Selected Intelligence Community Office of Inspector General Programs"

National Geospatial-Intelligence Agency (NGA) Office of Inspector General (OIG) Comments
To The Recommendations Regarding NGA-OIG

Recommendation 13: The Inspector General of NGA should establish specific timelines for completing investigations conducted by the Office of Inspector General of NGA.

NGA OIG Response: Concur. The NGA OIG will establish specific timelines for completing investigations. The timelines will include completion of major investigative milestones within 180 days of allegation receipt, i.e., initial review, planning, notifications, fieldwork, submittal of report to agency for action and notification to complainants. The NGA OIG will incorporate the timelines for completing investigations in the next version of NGA OIG's Investigations Handbook.

Recommendation 14: The Inspector General of NGA should develop and implement a quality assurance program for the OIG's Investigations Division. This program should consist of routine internal and external quality assurance reviews consistent with CIGIE standards and guidance.

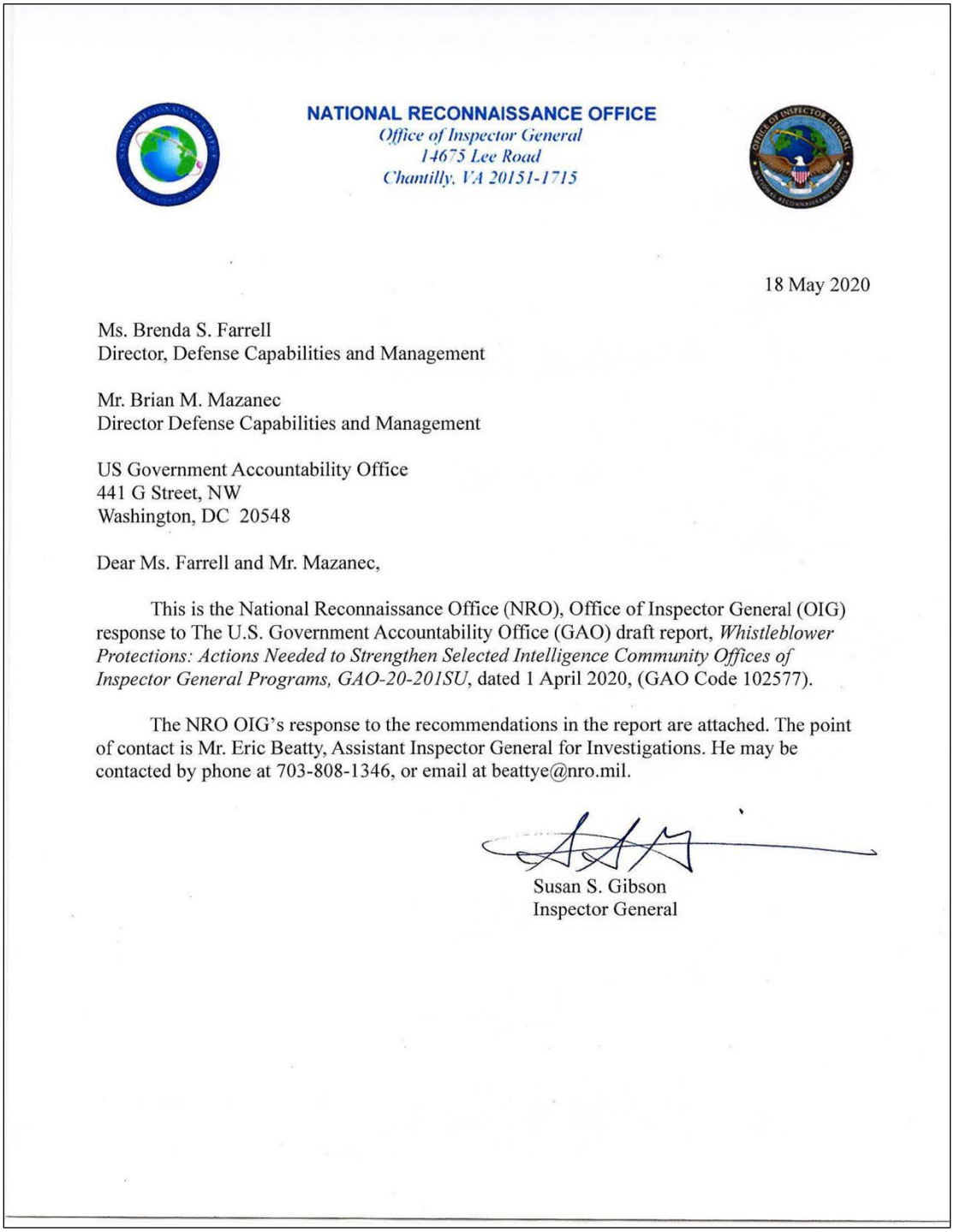
NGA OIG Response: Concur. The NGA OIG will develop a quality assurance checklist that is consistent with CIGIE standards and guidance for use internally by NGA OIG to evaluate the NGA OIG Investigations Division's program. The NGA OIG will set an objective to perform a routine internal quality assurance review every three years. NGA OIG will work with external CIGIE OIGs to conduct an external peer review of the Investigations Division that is consistent with CIGIE standards and guidance and performed every five years per CIGIE guidance.

Recommendation 15: The Inspector General of NGA should take steps to ensure that notifications to complainants in reprisal cases occur and are documented in the investigative case file, as required by OIG policy.

NGA OIG Response: Concur. By current policy, the notification and documentation is already required. Since the period under inspection, we have for the most part completed an initiative to move from hard-copy case files to an electronic case filing system. Under current closeout procedures, OIG Investigations Division management verifies the notification memo is in the case management tracking system before closing the case. However, as before, this is still a manual process. NGA OIG Investigations Division will work to determine if the current case management system can be modified to electronically notify management of the failure to document notification in reprisal cases.

UNCLASSIFIED

Appendix VIII: Comments from the Inspector General of the National Reconnaissance Office



NATIONAL RECONNAISSANCE OFFICE
Office of Inspector General
14675 Lee Road
Chantilly, VA 20151-1715

18 May 2020

Ms. Brenda S. Farrell
Director, Defense Capabilities and Management

Mr. Brian M. Mazanec
Director Defense Capabilities and Management

US Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Ms. Farrell and Mr. Mazanec,

This is the National Reconnaissance Office (NRO), Office of Inspector General (OIG) response to The U.S. Government Accountability Office (GAO) draft report, *Whistleblower Protections: Actions Needed to Strengthen Selected Intelligence Community Offices of Inspector General Programs, GAO-20-201SU*, dated 1 April 2020, (GAO Code 102577).

The NRO OIG's response to the recommendations in the report are attached. The point of contact is Mr. Eric Beatty, Assistant Inspector General for Investigations. He may be contacted by phone at 703-808-1346, or email at beattye@nro.mil.

Susan S. Gibson
Inspector General

National Reconnaissance Office, Office of Inspector General
Response to GAO Recommendations Cited in Whistleblower Protections: *Actions Needed to Strengthen Selected Intelligence Community Offices of Inspector General Programs*

GAO-20-201SU dated 1 April 2020

(GAO Code 102577)

Recommendation 16: The Inspector General of NRO should establish a time frame to finalize the OIG's draft investigations manual.
NRO OIG Response: Concur. The NRO OIG has established a date of 30 September 2020 on which to finalize its manual. The revised manual will incorporate, among other things, the investigative operating instructions previously used as a supplement to guidance and procedures provided in the manual.

Recommendation 17: The Inspector General of NRO should establish a process to regularly review and update the OIG's investigative procedures.
NRO OIG Response: Concur. The NRO OIG investigations manual will reflect that it will be reviewed at least every three years beginning with the period following the date that the current draft is finalized. The manual will also require an annual review to identify and incorporate any changes in law, regulation, and other policies relevant to investigative activities.

Recommendation 18: The Inspector General of NRO should continue to develop and implement a quality assurance program for the OIG's Investigations Division, which should consist of routine internal and external quality assurance reviews consistent with the CIGIE standards and guidance.
NRO OIG Response: Concur. The NRO OIG will continue to develop and implement its quality assurance program within the OIG's Investigations Division, and ensure the program's internal and external quality assurance reviews are conducted consistent with the CIGIE standards and guidance.

Recommendation 19: The Inspector General of NRO should consider making the use of documented investigative plans a requirement for all investigations.
NRO OIG Response: Concur. NRO OIG began using documented Investigative Plans more consistently in May 2018, and required documented investigative plans for all new cases starting October 2019. These changes are incorporated into the draft Investigations manual. The manual change requires the agent to create a documented case plan, which is reviewed by a Special Agent in Charge, and then used to brief OIG management during initial and recurring case reviews.

Recommendation 20: The Inspector General of NRO should revise its training plan to provide an approach that systematically links requisite knowledge, skills, and abilities to training reimbursements through an investigator's career progression.
NRO OIG Response: Concur. A matrix associating career progression to requisite knowledge, skills, abilities, and formal training has been developed and is awaiting final review by Human Resources for implementation in Fiscal Year 2021. The matrix identifies basic, advanced, and specialized training for progression from grade GS-11 to GS-15 and differentiates between investigators and investigative supervisors. The matrix also identifies minimum standards for advancement regarding investigative tradecraft, written and verbal communications, leadership, and understanding the intelligence mission. The matrix also accounts for the progression of non-supervisory senior agents with certain skill sets to include computer forensics, government contracting, and accounting.

Recommendation 21: The Inspector General of NRO should take steps to ensure that notifications to complainants in reprisal cases occur and are documented in the investigative case file as required by OIG policy.
NRO OIG Response: Concur. Chapter 13 of the draft NRO OIG investigations manual was amended in November 2019 to reflect that all complainants in reprisal cases will be notified in writing regarding the disposition of their case, as well as the process and details for requesting an external review, as appropriate. While the draft manual cites the need to retain documents and significant correspondence in all cases, that requirement has been repeated for emphasis in Chapter 13 regarding the notification to the complainant.

Appendix IX: Comments from the Inspector General of the National Security Agency

NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
OFFICE OF THE INSPECTOR GENERAL
9800 Savage Road, Suite 6247
Fort George G. Meade, MD 20755-6247

8 May 2020
IG-11941-20

Ms. Brenda Farrell
Mr. Brian M. Mazanec
Directors, Defense Capabilities Management
U.S. Government Accountability Office
441 G. Street, N.W.
Washington, DC 20548

Dear Ms. Farrell and Mr. Mazanec:

Thank you very much for the opportunity to provide the input of the National Security Agency Office of the Inspector General (NSA OIG) on draft U.S. Government Accountability Office (GAO) Report GAO-20-201SU, "Whistleblower Protection: Actions Needed to Strengthen Selected Intelligence Community Office of Inspector General Programs." This report discusses one of my office's highest priorities, and I very much appreciate your careful review and suggestions for improvement in this area. Enclosed are our comments on the draft report and recommendations.

Whistleblowers perform an invaluable service to the agencies where they work and the public at large when they come forward with what they reasonably believe to be evidence of wrongdoing. They should never suffer reprisal for doing so. These core principles are at the heart of our work here at the NSA OIG. Prior to being confirmed as the Inspector General here and coming on board at the start of 2018, I founded and chaired the Whistleblower Ombudsperson Working Group of the Council of the Inspectors General on Integrity and Efficiency (CIGIE), a responsibility that I continued to carry out as the Deputy Inspector General at the Department of Justice. In all of those efforts, I was guided by the seminal importance of whistleblowers for the work of the offices of the Inspectors General, and this has been at the forefront of my office's efforts here at the NSA.

In that regard, as detailed in our comments to the draft report, I have prioritized all reprisal matters at the NSA OIG, and I personally review every decision not to initiate a whistleblower reprisal investigation and every report of investigation on such matters. We have greatly expanded the information available to employees and others on whistleblower rights and protections, with designated pages on both our internal and our new external public facing website. We also have prepared a variety of materials and videos, and most recently provided the content for a training program on whistleblower rights and protections that at my request has been made mandatory for all agency employees. Additionally, shortly after coming on board, I created a new position, the

Whistleblower Coordinator, modeled on the Whistleblower Ombudsperson position that I held at DOJ, which has its own designated email address that employees and others within and outside the agency can contact to obtain additional information about their rights and protections. Additional information about my office's prioritization of whistleblower rights and protections and our activities in this area can be found in the Message from the Inspector General and Whistleblower Program sections in our Semiannual Reports to Congress, unclassified versions of which are available on our public website at https://oig.nsa.gov.

In terms of our own internal procedures, in addition to prioritizing whistleblower reprisal matters as described above, one major step that we have taken that I wish to highlight is that the OIG now affords complainants whose allegations we preliminarily have not substantiated an opportunity to review our tentative analysis and conclusions and to provide input for our consideration prior to finalizing the report. This helps to ensure not only the accuracy of our work, but also to enhance the sense of fairness and institutional justice that I believe is critical to our efforts in this area. In that regard, as noted in our comments on the draft, since we instituted this forward-leaning policy, we have had complainants whose allegations we have not substantiated indicate to us that while they were disappointed in the result, they appreciated the way in which the investigation was handled and the full opportunity they had to provide input during the process. Supporting whistleblower rights and protections does not mean substantiating every reprisal allegation; but it does mean taking them all seriously, reviewing them all carefully, and making every effort to make sure we reach the right result in a timely manner. We are committed to doing this at the NSA OIG, and again, we very much appreciate GAO's review as an opportunity to look at our efforts and pursue areas for improvement.

If you want to discuss any of our comments on the report or recommendations, or anything else on this matter, please do not hesitate to reach out to me, Assistant Inspector General for Investigations Kevin Gerrity, or Counsel to the Inspector General Andrew Snowdon, at (301) 688-6666.

Very truly yours,

Robert P. Storch
Inspector General

Enclosures
As indicated

UNCLASSIFIED

GAO Draft Report Dated May 2020
GAO-20-201SU

"Whistleblower Protection: Actions Needed to Strengthen Selected Intelligence Community Office of Inspector General Programs"

National Security Agency (NSA) Office of Inspector General (OIG)
Comments
On The Draft Recommendations Regarding NSA OIG

Recommendation 22: The Inspector General of NSA should develop and implement a quality assurance program for the OIG's investigation division. This program should consist of routine internal and external quality assurance reviews consistent with CIGIE standards and guidance.

NSA OIG Response: Concur. NSA OIG is expanding its internal Quality Assurance Program to encompass internal reviews for all divisions, including the Investigations Division. In addition, the new NSA OIG Assistant IG for Investigations is developing procedures that are consistent with CIGIE standards and guidance for: 1) continuous enhanced internal quality assurance reviews by the investigations division and 2) external peer reviews.

Recommendation 23: The Inspector General of NSA should develop an investigator training plan that provides an approach that systematically links the requisite knowledge, skills, and abilities to training requirements to an investigator's career progression

NSA OIG Response: Concur. The NSA OIG has always tailored training to the specific knowledge, experience, skills, and abilities of each investigator. In addition, NSA OIG Investigations Division personnel participate in weekly unit meetings and quarterly professional development. The new NSA OIG Assistant OIG for Investigations is preparing a formal training plan that incorporates such personalized training and development in a more systematic fashion, and a new monthly unit training plan is being developed as well.

UNCLASSIFIED

Appendix X: Comments from the Department of Defense

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

May 21, 2020

Ms. Brenda S. Farrell, Director
Defense Capabilities and Management
U.S. Government Accountability Office
441 G. Street, N.W.
Washington, DC 20548

Dear Ms. Farrell,

This responds to GAO's proposed report, "Whistleblower Protection: Actions Needed to Strengthen Selected Intelligence Community Offices of Inspector General Programs (GAO 20-201SU)." We thank the GAO for its careful review of the Department's Intelligence Community (IC) whistleblower protection programs and its professional interactions with our Office and the Defense IC Offices of Inspector General (OIGs).

On behalf of the Department of Defense, we concur with the report's recommendations concerning the Defense IC OIGs and stand ready to work with and assist them, as necessary, to implement the recommendations consistent with the DoD OIG's oversight authority and responsibilities. We offer no additional comment with respect to the specific recommendations, and our response neither supersedes nor supplants the responses provided to GAO by the Defense IC OIGs.

GAO's findings and recommendations are important to us, not only to enable the Defense IC OIGs to improve their efficiency and effectiveness, but also to ensure the implementation of processes to better protect whistleblowers and hold accountable those who would reprise against them.

Again, we thank the GAO for its contribution to the continuing improvement of the Department's whistleblower protection programs, as well as its professionalism during its engagement in this matter. If you have any questions, please contact the Primary Action Officer, David A. Core, Deputy General Counsel, at 703.604.8350.

Sincerely,

O'DONNELL.SEAN.WILLIAM.1589529886 Digitally signed by O'DONNELL.SEAN.WILLIAM.1589529886 Date: 2020.05.21 13:28:51 -04'00'

Sean O'Donnell
Acting Inspector General

Cc:
Inspector General, Defense Intelligence Agency
Inspector General, National Geospatial Intelligence Agency
Inspector General, National Reconnaissance Office
Inspector General, National Security Agency

Appendix XI: GAO Contacts and Staff Acknowledgments

GAO Contacts

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

Brian M. Mazanec, (202) 512-5130 or mazanecb@gao.gov

Staff Acknowledgments

In addition to the contact named above, Kimberly C. Seay (Assistant Director), Tracy Barnes, Katie Bassion, Adrianne Cline, Ryan D'Amore, Michele Fejfar, Neil Feldman, Samuel Harris, Chad Hinsch, James Krustapentus, Amie Lesser, Parke Nicholson, and Cheryl Weissman made key contributions to this report.

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 our website. Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. You can also subscribe to GAO's email updates to receive notification of newly posted products.

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 Email 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

Please Print on Recycled Paper.