

Defense Intelligence Agency Office of the Inspector General



Semiannual Report to Congress

October 1, 2019–March 31, 2020



Defense Intelligence Agency

Office of the Inspector General

Semiannual Report to Congress

1st and 2nd Quarters, FY 2020

Additional Information and Copies

This report and the annex are posted on the Joint Worldwide Intelligence Communications System and on the Secret Internet Protocol Router Network. A copy of this report can also be found on the Internet at <https://oig.dia.mil/> and at <http://www.oversight.gov>.

To request physical copies of this report, contact the DIA Office of Inspector General at (202) 231-1010.

Send us Your Audit and Inspection Suggestions

Defense Intelligence Agency

ATTN: Office of the Inspector General 7400 Pentagon

Washington, DC 20301-7400

**Are you aware of fraud, waste, or abuse
in a DIA program?**

If so, report it!

DIA Inspector General Hotline

Via phone

(202) 231-1000

Via email

ig_hotline@dia.mil

A Message From the Inspector General



I am pleased to present the Defense Intelligence Agency (DIA) Office of the Inspector General (OIG) semiannual report to the U.S. Congress covering the reporting period of October 1, 2019 through March 31, 2020. This report illustrates our oversight accomplishments and is a testament to my team's hard work, dedication, and resiliency.

In mid-March, I directed most of my staff to work from home to promote social distancing, health, and safety in response to the COVID-19 pandemic. Since much of our work relies on access to classified information and systems, teleworking has delayed our ability to complete some statutory requirements—including the semiannual report. Nevertheless, we released a Summary of Activity—a condensed version of our regular report—in April to keep the DIA and Congress fully and currently informed. We continue to significantly improve our remote capabilities and are taking a phased approach to expand our presence in the office.

Despite these delays, we have produced work that has benefited DIA, DoD, IC, and the American public. We engaged an independent public accounting firm to audit DIA's FY 2019 financial statements. The firm identified four material weaknesses and two significant deficiencies in the Internal Control report, and one instance in which DIA did not comply with Public Law 104-208, "Federal Financial Management Improvement Act of 1996," September 30, 1996. We also evaluated DIA's compliance with the Federal Information Security Modernization Act—reissuing three recommendations and issuing five new recommendations.

Additionally, we published 15 investigative reports. In four cases, we did not substantiate allegations of reprisal. We substantiated three cases regarding time and labor fraud, and one case regarding contractor cost mischarging; we estimated a \$112,451 loss to the Government. Additionally, we substantiated one case involving misuse of Government resources and one case involving abuse of authority and prohibited personnel practices. Further, we investigated but did not substantiate the allegations in five separate cases regarding use of public office for personal gain, misconduct, intelligence oversight, abuse of authority, and violations of the Privacy Act of 1974. Lastly, we issued eight management referral reports. In one referral, we recommended management take action to recoup \$40,544 in incentive payments to four DIA employees who improperly received them.

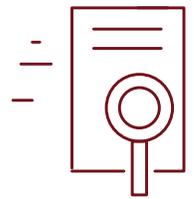
I would also like to highlight our ongoing efforts to improve our processes, fraud identification, data analytics and management, and information security. Our new Case Management and Tracking System will soon move into a production environment. Once fully operational, this system will replace three other databases and provide an efficient, reliable means to document and manage investigative cases. Lastly, we continue to work on the OIG Enterprise Risk Management program to identify, analyze, and mitigate internal and external risks that may impact our organization.

Although we are unsure when we will resume operations as they were, I am honored to lead such a talented, dedicated, and adaptive team. Regardless of the circumstance, their work continues to compel management action to achieve a more effective and efficient DIA Enterprise. I am also grateful for the continued support from the Director, DIA senior leaders, and Congress.



Kristi M. Waschull
Inspector General

Summary of Activity



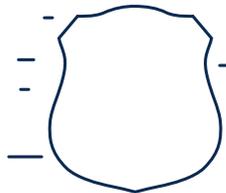
Audits

Reports Issued: 1
Material Weaknesses: 4
Significant Deficiencies: 2



Inspections & Evaluations

Reports Issued: 1
Recommendations: 8



Investigations

Reports Issued: 15
Recommendations: 11



Potential Cost Savings

Questioned Costs:

\$8.5 Million

Unsupported Costs:

\$5.2 Million

Funds Put to Better Use:

\$255 Million

Investigative Activity

Dollars Recovered

\$203,000

Description	Number
Cases Opened	21
Cases Closed	19
Referrals	15
Hotline Complaints	164

Case	Number
Abuse of Authority	2
Privacy Act Violation	1
Contractor Cost Mischarging	1
Misconduct	1
Reprisal	4
Use of Office for Personal Gain	1
Time and Labor Fraud	3
Misuse of Government Resources	1
Intelligence Oversight	1

Table of Contents

The DIA Office of the Inspector General.....	1
Office of the Inspector General Organization	2
Statutory Reporting.....	4
Summary of DIA Conference Reporting.....	5
Legislative and Regulatory Review	6
Summary of Audit Activity.....	7
Summary of Inspection and Evaluation Activity	8
Summary of Investigation Activity.....	9
Appendix A. Statistical Tables.....	15
Appendix B. Index of Reporting Requirements.....	19
Appendix C. Status of Recommendations.....	Annex¹
Appendix D. Audits, Inspections, and Investigations Closed Since Closed Since October 1, 2019.....	Annex

1. The Annex contains caveated and classified information, and therefore provided under separate cover.



The DIA Office of the Inspector General

The DIA Office of the Inspector General (OIG) is one of 73 Federal statutory Inspectors General (IGs) established by the IG Act of 1978, as amended. The IG Act contains provisions for OIG independence, the objectivity of OIG work, and safeguards against efforts to impair objectivity or hinder OIG operations.

Mission

Conduct independent, objective, and timely oversight across the Defense Intelligence Agency (DIA) Enterprise to promote economy; detect and deter fraud, waste, abuse, and mismanagement; and inform DIA and Congress. We accomplish this through independent audits, inspections, evaluations, investigations, and the OIG Hotline program.



Vision

Foster an inclusive and dynamic team of professionals that is a catalyst for accountability and positive change, compelling a more unified, adaptive, relevant, and agile DIA Enterprise.

Values

Teamwork

Collaboratively partner internally and across organizational boundaries to achieve common goals.

Integrity

Courageously adhere to the highest ethical principles and honor confidentiality, objectivity, and trustworthiness.

Excellence

Provide the highest quality products and customer service.

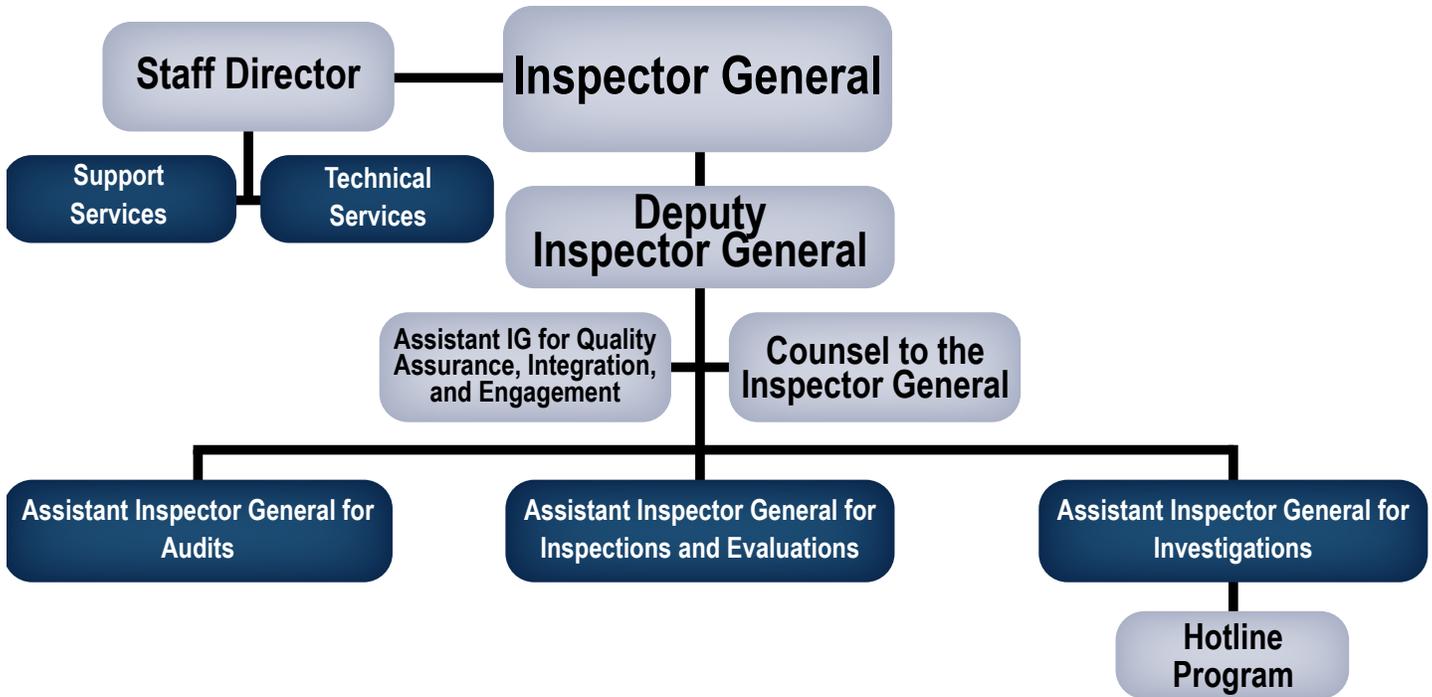
Accountability

Steadfastly commit to deliver solutions that meet the highest standards.

Initiative

Insightfully solve challenges and organize priorities.

Office of the Inspector General Organization



Audits

The Audits Division audits all aspects of DIA operations, providing recommendations that reduce costs; improve operational efficiency and effectiveness; strengthen internal controls; and achieve compliance with laws, regulations, and policy. It also conducts or oversees the annual independent audit of the Agency's financial statements.

Inspections and Evaluations

The Inspections and Evaluations Division evaluates the efficiency and effectiveness of DIA organizations, programs, and functions by conducting in-depth reviews across the Agency that examine and assess processes, procedures, internal controls, performance measures, compliance with regulatory and policy guidance, interrelationships, and customer satisfaction.

Investigations

The Investigations Division conducts proactive and reactive administrative and criminal investigations. Its primary objectives are to detect, deter, and report fraud, waste, and abuse within DIA; develop sufficient evidence to successfully resolve all allegations and facilitate successful criminal prosecution or management-directed disciplinary action; and identify and report internal control weaknesses that could render DIA programs and systems vulnerable to exploitation. The Investigations Division, in coordination with the DIA Office of the General Counsel, also reports and investigates questionable intelligence activities, as defined by Executive Order 12333, "United States Intelligence Activities," as amended.



Hotline Program

The Hotline Program is a confidential and reliable means for DIA employees and the public to report fraud, waste, mismanagement, and abuse of authority pertaining to DIA. The primary role of the program is to receive and evaluate concerns and complaints and determine the agency or responsible element best suited to take appropriate action.

Services

The Services Division manages all administrative programs and services directly supporting OIG. The Services Division enables useful audit, inspection, evaluation, and investigation activities and facilitates timely production of intelligence management and oversight products for DIA senior leadership and congressional overseers. Mission services functions include, but are not limited to, general counsel, quality assurance, manpower, budget, records management, correspondence, Freedom of Information Act and Privacy Act, security, planning, training, information systems, and data analytics in support of the OIG mission.



A Bangkok-based Defense Attaché Service C-12 aircraft delivers Meals Ready to Eat for the youth soccer team trapped in the Tham Luang Nang Non cave in Chiang Rai Province, Thailand.

Statutory Reporting

Reports to the Director of Refusal to Provide Information

Section 5(a)(5) of the IG Act of 1978 requires IGs to promptly report to the head of the establishment if information requested is unreasonably refused or not provided. No such reports were made during this reporting period.

Reports Previously Issued That Lacked Management Comment Within 60 Days

Section 5(a)(10)(B) of the IG Act of 1978, as amended by the IG Empowerment Act, requires IGs to provide a summary of each audit, inspection, and evaluation report issued prior to the current reporting period for which no establishment comment was returned within 60 days of delivery of the report. No such reports were made during this reporting period.

Significant Revised Management Decisions

Section 5(a)(11) of the IG Act of 1978 requires IGs to describe and explain the reasons for any significant revised management decisions made during the reporting period. We are not aware of revisions to any significant management decisions during this reporting period.

Significant Management Decisions With Which the IG Disagrees

Section 5(a)(12) of the IG Act of 1978 requires IGs to provide information concerning any significant management decisions with which they disagree. During this reporting

period, there were no instances in which the IG disagreed with significant management decisions.

Federal Financial Management Improvement Act of 1996

Section 5(a)(13) of the IG Act of 1978 requires IGs to provide information described under section 804(b) of the Federal Financial Management Improvement Act of 1996. This information involves the instances and reasons when an agency has not met target dates within its remediation plan to bring financial management systems into compliance with the law. In Fiscal Year (FY) 2018, DIA re-assessed its noncompliance with Federal financial management system requirements, and developed and implemented updated remediation plans to address areas of noncompliance. The Agency has not missed any of its remediation plan target dates.

Attempts to Interfere With the IG's Independence

Section 5(a)(21) of the IG Act of 1978, as amended by the IG Empowerment Act, requires IGs to provide detailed descriptions of any attempts by their establishments to interfere with their independence. We did not experience any attempts to interfere with our office's independence during this reporting period.

Public Disclosure

Section 5(a)(22) of the IG Act of 1978, as amended by the IG Empowerment Act, requires IGs to provide detailed descriptions of inspections, evaluations, audits, and investigations involving senior Government employees that were

closed during the reporting period without being publicly disclosed. Summaries of all such work are included in the appropriate sections of this report.

Peer Reviews

Sections 5(a)(14–16) of the IG Act require IGs to report information about peer reviews that their offices have been subject to, including any recommendations that have not been fully implemented and a justification as to why. We were not subject to any peer reviews this reporting period. However, on November 6, 2017, the National Geospatial-Intelligence Agency OIG completed a peer review of our Inspections and Evaluations covering the preceding 3 years. All recommendations were implemented. Furthermore, on April 30, 2017, the Central Intelligence Agency completed a peer review of our Audits covering the preceding 3 years. We implemented all recommendations. We are currently conducting an audit peer review of the National Reconnaissance Office and will include the results in a future semiannual report (SAR).

National Defense Authorization Act of FY 2020

Section 6718(b) of the National Defense Authorization Act of Fiscal Year 2020 requires IGs to report the number of investigations regarding unauthorized public disclosures of classified information to congressional intelligence committees, to include the number of reports opened, closed, and referred to the Attorney General for criminal investigation. We did not open, close, or refer any such investigations this reporting period.

Summary of DIA Conference Reporting

Section 738 of the Consolidated Appropriations Act of 2019 requires the heads of executive branch organizations to provide certain details to the IG regarding the organization’s involvement in conferences. The table below represents reported conference costs with totals that exceed the reporting threshold of \$20,000. Most reported costs are estimates. We have not verified the accuracy or completeness of the data reported below; calculations are done by the appropriate Agency points of contact.

Conference Name	Type	Estimated Cost	Actual Cost
Gartner Reimagine HR Conference	Non-DoD-hosted	\$31,530	Pending
2019 DIA Activity Workshop	DIA-hosted	\$73,354	\$72,956.33
FY 2019 Global Summit	DIA-hosted	\$483,747	Pending
2020 Coordinator Seminar	DIA-hosted	\$87,670	Pending
2020 DIA Activity Conference- Europe Region	DIA-hosted	\$68,769	Pending
EO Strategy Offsite	DIA-hosted	\$42,079	Pending
2020 DoD Conference	DIA-hosted	\$237,524	Pending
2020 DIA Activity Conference-Europe Region	DIA-hosted	\$74,694	Pending
FY 2020 DIA Activity Conference	DIA-hosted	\$138,737	Pending
CISCO Live 2020, Barcelona	Non-DoD-hosted	\$22,580	\$20,987
RSA Conference 2020	Non-DoD-hosted	\$48,235	Pending
CSUN Assistive Technology Conference	Non-DoD-hosted	\$28,724	Pending
Total		\$1,337,643	–



The Directors of Intelligence panel discussion at the 2019 Defense Intelligence Agency DoDIIS Worldwide Conference.

Legislative and Regulatory Review

Section 4(a) of the IG Act of 1978 requires IGs to review existing and proposed legislation and regulations relating to the programs and operations of their respective organizations. Our reviews include legislation, executive orders, memorandums, directives, and other issuances. The primary purpose of our reviews is to assess the impact of proposed legislation or regulations on the economy and efficiency of programs and operations administered or financed by DIA, or the potential for fraud and abuse in these programs. During the reporting period, we reviewed proposed changes to the following:

Description	Number Reviewed
Legislation	13
Department of Defense Issuances	38
Defense Intelligence Agency Issuances	31
Office of the Director of National Intelligence Issuances	0
Executive Orders	0





Defense Intelligence Agency Financial Statement Audit for Fiscal Year 2019, Project 2019-1004

We engaged an independent public accounting (IPA) firm to audit DIA’s FY 2019 financial statements. The firm did not issue an opinion because the general property, plant, and equipment were not properly recorded in accordance with U.S. generally accepted accounting principles. In addition, unresolved accounting issues and material weaknesses limited DIA’s ability to promptly provide sufficient evidential support. The IPA identified four material weaknesses and two significant deficiencies.

Material Weaknesses:

- Information technology controls and financial systems.
- Identifying, correcting, and remediating deficiencies in controls to prevent accounting errors or financial misstatements.
- Enhancing data quality to enable sufficient retrieval of accounting transaction documentation.
- Property, plant, and equipment.

Significant Deficiencies:

- Oversight and monitoring of third-party service providers.
- Controls over accounting data transfers.



However, the IPA also noted that DIA management’s remediation activities were evident and that management continued to enhance efforts to implement process improvements.

Other Audit Activity

We closed 5 of the 19 open recommendations listed in our last report and continued to coordinate with Agency management to develop corrective action plans for the remaining recommendations.² At the end of the reporting period, we were in the process of finalizing reports for DIA’s IT services contracts and controls for removal of access for out-processing individuals.³ We are continuing our oversight of the audit of DIA’s FY 2020 financial statements and conducting fieldwork for projects regarding unplanned price changes, improper payments, and the Federal Information Security Modernization Act (FISMA) of 2014. Due to the COVID-19 pandemic, we have delayed our audit of emergency and extraordinary expenses. We expect to report the results of our audits of IT services contracts, access removal, and improper payments in the next SAR.

2. The Fall 2019 SAR indicated that DIA had 17 open audit recommendations at the end of the reporting period. However, the closure of two recommendations for Project 2007-1005 were not reported.

3. These reports have since been issued and will be reported in our next SAR.

Inspections & Evaluations

Evaluation of DIA's Compliance with the Federal Information Security Modernization Act, Project 2019-2005

The purpose of FISMA is to strengthen information security by requiring agency leaders to reduce information system security risks to an acceptable level and in a cost-effective manner. The Act requires each Federal agency to develop, document, and implement an agency-wide information security program to protect information and systems, including those provided or managed by another agency, contractor, or other source. We found that the DIA Chief Information Office made progress in addressing network risks and previous FISMA recommendations; however, we reissued three recommendations and issued five new recommendations.

Other Inspection and Evaluation Activity



This reporting period, we closed two recommendations. We remain engaged with Agency stakeholders and managers on progress and actions to satisfy the 25 open recommendations. At the end of the reporting period, we had issued the draft report of our evaluation of DIA's Special Access Program and were awaiting management comments.⁴ Additionally, we have decided to suspend our inspection of DIA's electronic record management due to significant overlap with the 2019 National Archives and Records Administration (NARA) inspection. Our decision to continue with the record management inspection is contingent upon NARA's final inspection report. We are also continuing work on our evaluations of the Foreign Disclosure Office and the Agency's use of classification markings. We will report the results of these projects in future SARs.

4. This report has since been issued and will be reported in our next SAR.



Investigative Activity Overview

Reprisal Investigations

We completed four investigations involving allegations of reprisal made before October 1, 2019.⁵ We determined that there was insufficient evidence to support the allegations of reprisal in all four cases. This reporting period, we received 10 reprisal complaints from DIA personnel: 8 did not meet the elements of reprisal, and 2 are under active investigation by our office.⁶

Time and Labor Investigations

We investigated three cases involving time and labor fraud by three DIA employees. We substantiated all allegations and identified a \$24,326.83 loss to the Government. All three cases represented a violation of Federal statute and were referred to the Office of the Assistant U.S. Attorney for the Western District of Virginia and the District of Columbia; both declined to prosecute. However, the DIA Office of the Chief Financial Officer issued letters of indebtedness to recover the loss.

Abuse of Authority Investigations

We investigated two abuse of authority cases involving two senior DIA senior officials. In the first case, we received an allegation that a senior official wrongfully excluded another DIA senior official from serving as a panel member on a hiring board. We determined there was insufficient evidence of abuse of authority and unethical behavior against the DIA senior official. In the second case, we substantiated allegations of prohibited personnel practices and abuse of authority against a DIA senior official. We determined the senior official leveraged their position of authority and advocated for DIA to hire their family member and abused their authority when they used their position for private gain.

Employee Misconduct Senior Military Official Investigation

We investigated an allegation that a DIA senior military official made disparaging comments regarding sex, race, and sexual preference of U.S. Embassy personnel. We determined there was insufficient evidence that the senior military official violated any provisions of the Uniformed Code of Military Justice.

5. Summaries of these cases are provided in our “Summaries of Published Investigative Reports” (2019-5008-OI, 2019-5016-OI, 2019-5017-OI, and 2019-5035-OI) starting on page 11 of this report.

6. The three elements of reprisal are defined by Presidential Policy Directive 19 (PPD-19), “Protecting Whistleblowers with Access to Classified Information,” or by title 10, United States Code, section 1034, “Protected communication; prohibited of retaliatory personnel actions,” updated December 12, 2017, for civilian and military complainants, respectively.

Misuse of Government Resources Investigation

We substantiated an allegation of misuse of Government resources by a DIA senior official. We determined the senior official used Government IT systems for their personal real estate business and to access sexually explicit and violent content while on official duty. We also determined the senior official violated Agency policy when they failed to report and obtain approval for outside employment.

Privacy Act Violation Investigation

We substantiated allegations against a DIA employee who violated the Privacy Act of 1974 and DoD Regulation 5400.11-R, "Department of Defense Privacy Act Program," May 14, 2007, when the employee released information about another former DIA employee to a foreign national and an attorney outside DoD.

Intelligence Oversight Investigation

We did not substantiate an allegation that a DIA organization misused intelligence information to take an administrative action against a DIA employee. The employee was suspended because the employee was the subject of a security investigation conducted by another agency.

Other Investigative Activities

During this period, we substantiated allegations of cost mischarging by a DIA contractor employee; the contract company reimbursed the Government \$106,422 and the contractor's employment was terminated. Additionally, we referred an anonymous complaint involving four DIA employees who received relocation incentives without relocating. We referred the complaint to Agency management who determined the employees were initially entitled to the relocation incentives. However, because they did not follow the agreed upon guidance, they were not entitled to the relocation incentives.

Investigative Activities⁷

Description	Quantity
Cases Opened in Reporting Period	21
Cases Closed in Reporting Period	19
Cases Still Open at End of Reporting Period	45
Investigation Reports Issued in Reporting Period ⁸	15
Referrals in Reporting Period (Number of Cases)	15
Referred to Management (Number of Cases)	7
Referred to Prosecutorial Authority (Number of Cases)	1
Number of Persons Referred to Department of Justice for Criminal Prosecution	0
Number of Persons Referred to State or Local Prosecuting Authorities for Criminal Prosecution (includes military authorities)	1
Total Number of Indictments and Criminal Informations Resulting from Prior Referral to Prosecuting Authorities	1

7. Description of Metrics: all metrics provided were developed as a result of reviewing all relevant individual cases including those opened and closed during this reporting period, and cases remaining open at the end of the previous reporting period (April 1, 2019–September 30, 2019).

8. One of the 15 cases issued during the reporting period (2019-5083-OI) involved Intelligence Oversight. This case was closed; however, one Intelligence Oversight case (2018-5006-OI) remains open pending management response.

Summaries of Published Investigative Reports

Use of Office for Personal Gain, Case 2018-5056-OI

We did not substantiate allegations that a DIA employee used their official position for personal gain or that Government funds were wasted by purchasing nonexistent IT software. Based on the evidence, we determined that the employee did not violate title 5, Code of Federal Regulations (C.F.R.), section 2625.502 (5 C.F.R. § 2625.502), “Personal and business relationships,” or 5 C.F.R. § 2635.702, “Use of public office for private gain.” We also determined that DIA legitimately purchased trademarked IT software in support of a current Agency contract.



Reprisal, Case 2019-5008-OI

We did not substantiate allegations of reprisal made by a former DIA contractor employee, who alleged that a DIA senior official retaliated against them for making a complaint against the official’s friends and two other DIA senior officials, one of which is retired. Specifically, the former contractor employee alleged the senior official had them removed from a DIA contract and influenced their company program manager to propose their termination. We determined evidence was insufficient to conclude the senior official acted in retaliation. We later concluded that the contractor employee and the contract company made an agreement that resulted in the contract employee’s resignation.

Reprisal, Case 2019-5016-OI

A former DIA employee alleged that they were retaliated against and improperly terminated by a supervisory DIA employee. The employee reported they were terminated in retaliation for filing claims of workplace harassment against the supervisory DIA employee and other coworkers. There was insufficient evidence to conclude the supervisory employee engaged in the prohibited personnel practice of reprisal, abuse of authority, or gross mismanagement. We determined the employee was terminated during their probationary period because of their performance. The steps to terminate the employee began prior to their complaint.

Reprisal, Case 2019-5017-OI

We did not substantiate allegations that two DIA supervisory employees committed acts of reprisal. A DIA employee alleged that one of the supervisory employees instructed them not to further report an incident involving prostitution and U.S. Government personnel in a deployed environment. The employee further claimed that their annual performance rating was downgraded, and they were prohibited from future deployments in retaliation for reporting the incident. The employee also alleged that the other supervisory employee, along with the first, further retaliated against them by downgrading their promotion packet. We determined there was insufficient evidence to conclude that the supervisory employees engaged in the prohibited personnel practice of reprisal, or otherwise engaged in retaliation, abuse of authority, or gross mismanagement.

Abuse of Authority, Case 2019-5024-OI

We did not substantiate allegations of abuse of authority and unethical behavior against a DIA senior official. We were notified that the senior official wrongfully excluded a DIA employee from serving as a panel member for a selection board. We determined evidence was insufficient to conclude that the senior official abused their authority or otherwise engaged in unethical behavior. The DIA senior official acted in good faith with the information provided to them.

Privacy Act Violation, Case 2019-5025-OI



We substantiated allegations that a DIA employee violated the Privacy Act of 1974 and DoD Regulation 5400.11-R, “Department of Defense Privacy Program,” May 14, 2007, when the employee released information about another DIA employee to a foreign national and an attorney outside DoD. However, we determined that the employee did so unknowingly. The employee believed the foreign national was an officer of the court, and the employee coordinated with Agency officials for guidance before releasing the information. The employee received a Letter of Counseling because of the violations.

Reprisal, Case 2019-5035-OI

We did not substantiate allegations of reprisal made by a DIA employee against a supervisory DIA employee. The employee alleged that their supervisor removed them from a special access program and threatened to deny their leave in retaliation for making a protected communication to their chain-of-command. We determined that the supervisory employee did not violate title 10, United States Code, section 1034, “Protected communications; prohibition of retaliatory personnel actions,” or Presidential Policy Directive-19 “Protecting Whistleblowers with Access to Classified Information.” In addition, we determined that the employee was removed from the program based on mission requirements.

Time and Labor Fraud, Case 2019-5042-OI

We substantiated allegations of time and labor fraud, false official statements, false claims, and theft of Government funds against a DIA employee. The employee failed to comply with DIA time and labor issuances when they knowingly prepared, signed, and submitted fraudulent time and labor records from July 22, 2018 to April 5, 2019, totaling 58.52 hours that they did not work. We estimated a \$3,154.21 loss to the Government. Since this case represented a violation of law, it was referred to the Assistant U.S. Attorney (AUSA), who declined to pursue prosecution. Ultimately, the Agency was paid the amount lost, and the employee resigned.

Contractor Cost Mischarging, Case 2019-5045-OI

We substantiated allegations of false official statements, false claims, and theft of public funds against a former DIA contractor employee. We determined that between 2017 and 2019, the contractor prepared and submitted fraudulent timesheets claiming approximately 776 hours that they did not work. We estimated a \$88,120.16 loss to the Government. However, after further examination, the contract company estimated the loss to the Government to be \$102,422.47, and reimbursed the full amount. Since this case represented a violation of law, it was referred to the AUSA, who declined to pursue prosecution.

Time and Labor, Case 2019-5056-OI

We substantiated allegations of time and labor fraud, false official statements, false claims, and theft of Government funds by a DIA employee. The employee failed to comply with DIA time and labor issuances when they knowingly prepared, signed, and submitted fraudulent time and labor records from June 10, 2018 to May 25, 2019. We determined a \$12,550.19 loss to the Government. Since this case represented a violation of law, we referred this case to the AUSA, who declined to prosecute. Disciplinary action against the employee is pending.

Time and Labor Fraud, Case 2019-5065-OI

We substantiated allegations of time and labor fraud, false official statements, false claims, and theft of Government funds against a DIA employee. We determined the employee signed and submitted fraudulent labor records between May 27, 2018, and June 22, 2019, totaling 110.13 regular hours that they did not work. Additionally, the employee claimed 18.34 compensatory hours and 29.31 credit hours that were unaccounted for. We estimated an \$8,627.43 loss to the Government. Since the case represented a violation of law, we referred it to the AUSA, who declined to prosecute. Disciplinary action against the employee is pending.

Misuse of Government Resources, Case 2019-5066-OI

We substantiated allegations of misuse of Government resources against a DIA senior official. The official used Government IT systems to complete work for their real estate business and to access sexually explicit and violent content while on official duty. We also determined the employee violated Agency policy that requires employees to report and obtain approval for outside employment. Disciplinary action is pending.

Abuse of Authority and Misuse of Government Resources (Prohibited Personnel Practices), Case 2019-5069-OI

We substantiated allegations of prohibited personnel practices and abuse of authority against a DIA senior official. We determined the senior official leveraged their position of authority and advocated for DIA to hire their family member. Further, we determined the senior official abused their authority and developed personal and business relationships for private gain by establishing an Agency outreach program that benefited that same family member's university and a private organization that the member led. Since this case represented a violation of law, we referred it to the AUSA, who declined to prosecute. Disciplinary action against the official is pending.

Employee Misconduct, Case 2019-5077-OI

We investigated allegations of misconduct against a DIA senior military official. Specifically, it was alleged that the military official made disparaging comments regarding sex, race, and sexual preference of U.S. Embassy personnel while in an official capacity. We determined the military official did not violate any provision of the Uniform Code of Military Justice, rule, or regulation; engage in any conflict of interest; or abuse their authority.

Intelligence Oversight, Case 2019-5083-OI

We did not substantiate an allegation that a DIA organization misused intelligence information to take an administrative action against a DIA employee. The organization suspended the employee's access because the employee was the subject of an investigation involving security matters. The organization was within its authority to suspend access while the investigation was ongoing.

Significant Management Referral

Allegations of Unauthorized Receipt of Incentive Pay, Case 2019-5074-WA

We received a complaint that alleged four DIA employees at an overseas location had inappropriately received relocation incentive bonuses for relocating to a new duty station within the same country they currently worked. We referred the matter to DIA management, who determined the employees were authorized to receive a relocation bonus; however, they never executed permanent transfers resulting in a \$40,544 loss to the Government.

Investigative Activity Support

Personnel Vetting

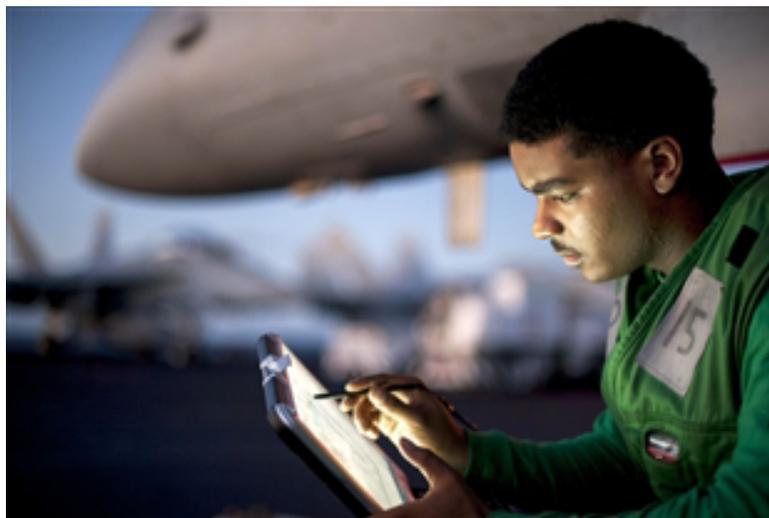
This reporting period, we completed 1,876 checks for derogatory information within OIG records in response to 128 requests, which originated within DIA. These requests involved DIA military and civilians who are seeking job placement or advancement, or are under consideration for awards.



Appendix A. Statistical Tables

Table A-1: Audit and Inspection Reports With Questioned and Unsupported Costs

Description	Number of Reports	Questioned Costs	Unsupported Costs
Reports for which no management decision was made by beginning of reporting period	3	\$8,458,936	\$5,182,720
Reports issued during reporting period	–	–	–
Reports for which a management decision was made during reporting period			
1. Dollar value of disallowed costs	–	–	–
2. Dollar value of allowed costs	2	\$7,926,508	\$4,650,292
Reports for which no management decision was made by the end of the reporting period ⁹	1	\$532,428	\$532,428
Reports for which no management decision was made within 6 months	1	\$532,428	\$532,428



Aviation Structural Mechanic inspects a F/A-18C Hornet schematic aboard aircraft carrier USS Carl Vinson.

9. Audit of DIA's Contract Surveillance, Project 2013-100010-OA: Published in DIA OIG Semiannual Report to Congress April 1, 2015–September 30, 2015. We found that DIA contracting officials and requiring activity personnel did not provide sufficient technical oversight to ensure that contractors performed in accordance with contract specifications. As a result, DIA had limited assurance that \$373.8 million in services and supplies met contract requirements. We also identified \$532,428 in unsupported costs for travel, tuition, and housing claimed under ODC in the invoices that were reviewed. Management analyzed most of the unsupported costs but have not completed their review.

Table A-2: Audit and Inspection Reports With Recommendations That Funds Be Put to Better Use

Description	Number of Reports	Funds to be Put to Better Use
Reports for which no management decision was made by the beginning of reporting period	2	254,770,000
Reports issued during reporting period	–	–
Reports for which a management decision was made during reporting period		
1. Dollar value of recommendations agreed to by management	–	–
2. Dollar value of recommendations not agreed to by management	–	–
Reports for which no management decision was made by the end of the reporting period ^{10, 11}	2	254,770,000
Reports for which no management decision was made within 6 months	2	254,770,000

Table A-3: Investigations Dollar Recoveries in Reporting Period

INVESTIGATION	CASE NUMBER	EFFECTIVE RECOVERY DATE	DOLLARS RECOVERED
Time and Labor Fraud and False Claims	2016-5081-OI	26 February 2020	\$25,831.69
Time and Labor Fraud and False Claims	2017-5068-OI	8 October 2019	\$16,482.83
Time and Labor Fraud and False Claims	2019-5042-OI	2 March 2020	\$3, 129.01
Contractor Cost Mischarging ¹²	2019-5045-OI	17 January 2020	\$106,422.47
Time and Labor Fraud and False Claims	2019-5056-OI	30 January 2020	\$10,488.02
Relocation Incentive Bonus	2019-5074-WA	10 March 2020	\$40,793.00
Total			\$203,147.02

10. Audit of Indefinite-Delivery/Indefinite-Quantity (IDIQ) Contracts, Project 2016-1004: Published in DIA OIG Semiannual Report to Congress April 1, 2017–September 30, 2017. We found that the Office of the Chief Financial Officer, Contracting Operations Division, could not determine the timeliness of IDIQ contract awards because it did not consistently establish contract milestones or record completion dates. As a result, DIA awarded six IDIQ contracts 3–5 months later than planned, and the delay for one contract increased the ceiling price by \$4.77 million. Management agreed with the corresponding recommendations.

11. Audit of DIA’s Unliquidated Obligations, Project 2017-1006: Published in DIA OIG Semiannual Report to Congress April 1, 2018–September 30, 2018. We found that DIA was unlikely to spend about \$250 million of its FY 2017 appropriations, in spite of obligating nearly all funds. Management has closed four of the corresponding recommendations and is working on the remaining three open recommendations.

12. Our Investigation estimated a loss of \$88,120.16; however, the contracting company’s audit estimated a higher loss and reimbursed at the higher rate. The dollar amount represents the total reimbursement.

Table A-4: Other Investigative Matters

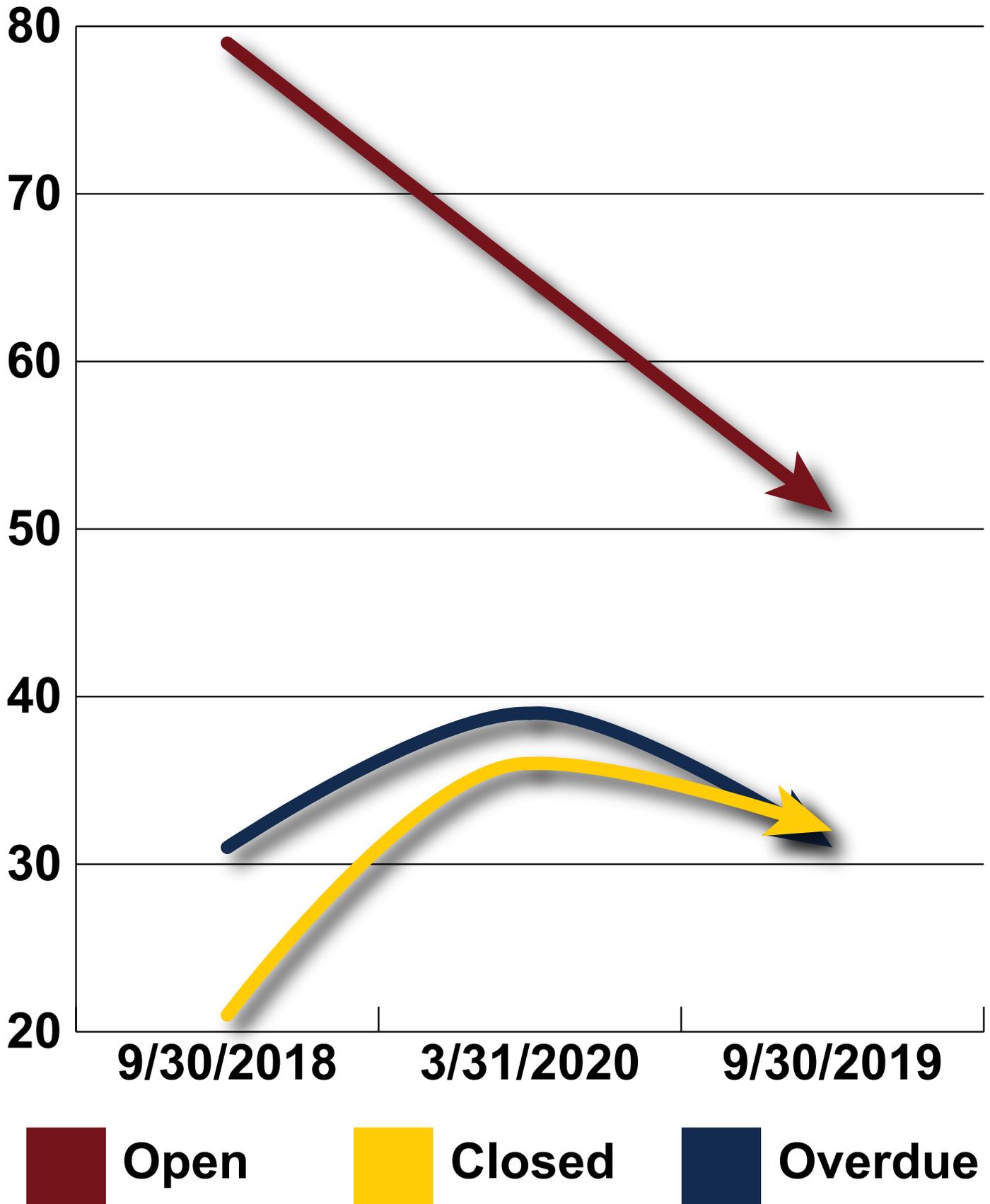
Description	Quantity
Hotline Program	
DIA OIG Hotline Inquiries Received in Reporting Period	172
DIA OIG Hotline Inquiries Closed in Reporting Period	121
Intelligence Oversight	
Cases Opened in Reporting Period	0
Cases Closed in Reporting Period	0
Cases Still Open at End of Reporting Period	1
Reports of Investigation Issued in Reporting Period	0
Referred to Management	0
Management Referrals	
Referrals in Reporting Period	8
Referrals in Reporting Period (external agencies)	1

Table A-5: Summary of Recommendations as of March 31, 2020¹³

DESCRIPTION	QUANTITY
Audits	
Open Recommendations	14
Closed Recommendations	5
Overdue Recommendations	14
Inspections	
Open Recommendations	25
Closed Recommendations	2
Overdue Recommendations	15
Investigations	
Open Recommendations	6
Closed Recommendations	5
Overdue Recommendations	6

13. "Overdue recommendations" refers to those recommendations that DIA management has not addressed within established timelines.

Table A-6: Recommendation Trends



Appendix B. Index of Reporting Requirements

Semiannual Reporting Requirement		Page
4(a)(2)	Legislative and regulatory reviews	6
5(a)(1)	Significant problems, abuses, and deficiencies	7–14
5(a)(2–3)	Recommendations to correct significant problems, abuses, and deficiencies	Annex
5(a)(4)	Matters referred to prosecutive authorities and resulting prosecutions and convictions	10–14
5(a)(5)	Reports to the Director, DIA of refusals to provide information	4
5(a)(6)	List of reports issued during the reporting period	7–14
5(a)(7)	Summaries of significant reports	7–14
5(a)(8)	Statistical table showing questioned and unsupported costs	15
5(a)(9)	Statistical tables showing recommendations that funds be put to better use	16
5(a)(10)(A)	Summaries of reports previously issued that still lack management decision	15–16
5(a)(10)(B)	Summaries of reports previously issued that lacked management comment within 60 days	4
5(a)(10)(C)	Summaries of reports previously issued that have remaining unimplemented recommendations	Annex
5(a)(11)	Significant revised management decisions	4
5(a)(12)	Significant management decisions with which the IG disagrees	4
5(a)(13)	Federal Financial Management Improvement Act of 1996	4
5(a)(14–16)	Peer reviews	4
5(a)(17–18)	Investigations statistics and metrics	10
5(a)(19)	Investigations involving substantiated allegations against senior officials	9–14
5(a)(20)(A)	Descriptions of whistleblower retaliation	9–14
5(a)(20)(B)	Establishment imposed consequences of whistleblower retaliation	9–14
5(a)(20)(C)	Whistleblower retaliation settlement agreements	9–14
5(a)(21)	Attempts to interfere with IG independence	4
5(a)(22)	Public disclosure	4
6718(b)	National Defense Authorization Act of FY 2020	4



Soldiers enjoy a brief rest during the ARCYBER Best Warrior Competition at Marine Corps Base Quantico.

