DEFENSE INTELLIGENCE AGENCY

Office of the Inspector General

Summary of Activity

October 1, 2019–March 31, 2020

A Message from the Inspector General

I am pleased to present a summary covering the oversight activities of the Office of the Inspector General (OIG) for the Defense Intelligence Agency (DIA) from October 1, 2019, to March 31, 2020. In mid-March, I directed most of our employees to telework from home to promote social distancing consistent with national, Intelligence Community (IC), Department of Defense (DoD), and Agency guidelines. We uphold a small oversight presence onsite to cover our most essential functions—all other activities are maintained through teleworking.

Much of our work relies on access to classified information and systems and through engagement with Agency and community counterparts. Teleworking severely limits or restricts our access and engagement. As a result, we are unable to publish a comprehensive Semiannual Report (SAR) to Congress; however, we have produced work that has benefited DIA, DoD, IC, and the American public.

Despite production for this reporting period halting due to the pandemic, we issued one audit and one inspection report, outlining insights and recommendations accepted by management. Additionally, we completed 15 investigations and eight management referral reports identifying management actions, and estimated $152,995 losses due to fraud, waste, and abuse. Much of our work during this reporting period focused on the top management and performance challenges facing the Agency, including financial management and oversight of contracts. We also worked with management to close several recommendations. The following are additional details regarding our oversight work.

Audits: We engaged an independent public accounting firm to audit DIA's FY 2019 financial statements. The report was issued in November 2019. 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 oversaw this work based on standards and supported the DoD OIG department-wide audit. We currently have five ongoing audits including IT Service Contracts, Access Removal, Unplanned Price Changes, Emergency and Extraordinary Expenses, and an Improper Payments Elimination and Recovery Act (IPERA) evaluation. In addition, we have one other audit in pre-announcement planning. During this reporting period, we closed the audit of Other Direct Costs; we also closed five audit recommendations and 14 remain open. In addition, we are also conducting a peer review of the National Reconnaissance Office. We plan to include the results of the IT Services Contracts audit, Access Removal audit, and the peer review in our fall SAR.

Inspections and Evaluations: We evaluated DIA's compliance with the Federal Information Security Modernization Act—reissuing three recommendations and issuing five new recommendations. We also have five ongoing projects. We issued a draft evaluation of Special Access Program Central Office for management comment. We also announced evaluations of Foreign Disclosure and Classification Management. We fully expect to finish all three projects by the end of FY 2020 for reporting in the fall SAR. In addition, we have two other projects in pre-announcement planning that will be included in future SARs. We have 25 open recommendations. During the reporting period, we added five new recommendations and closed two.

Investigations: During the reporting period, we published 15 investigations. Four cases involved unsubstantiated allegations of reprisal. In three cases, we substantiated time and labor fraud allegations with

an estimated loss of $24,331 to the Government. One case, regarding allegations of contractor cost mischarging, was substantiated with an estimated $88,120 loss to the Government. We also substantiated one case involving misuse of Government resources and another case involving abuse of authority coupled with prohibited personnel practices. Further, we investigated a case involving the use of public office for personal gain, in which we determined evidence was insufficient to conclude a violation occurred. Four other unsubstantiated cases involved allegations of misconduct by a senior military official, misuse of intelligence information for administrative actions against an employee, abuse of authority by a senior official, and violations of the Privacy Act of 1974. Lastly, in other investigative activity, we issued eight management referral reports. In one referral, we recommended management take action to recoup $40,544 in incentive pay to four DIA employees; the employees were approved for and received incentive pay but did not execute the incentive pay action.

I would also like to highlight our ongoing efforts to improve our oversight processes and enhance data management and security. We continue to expand our proactive fraud investigative resources and data analytic capabilities. Additionally, we are still on track to deploy our new Case Management and Tracking System, and we initiated planning for an OIG enterprise risk management program. Through risk management, we will identify and examine specific internal risks that affect our organization, and we will plan and execute strategies to mitigate these risks. Equally important, the program will also help us analyze and make recommendations to address internal enterprise risk management on a permanent basis.

Our accomplishments reflected in this summary are a credit to the talented and dedicated staff that I have the privilege to lead. We are committed and look forward to delivering the SAR with classified annex, as required by statute, upon resuming normal operations.

Kristi M. Waschull
Inspector General

Summary of Audit Activity

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

We engaged an independent public accounting firm, Ernst and Young (E&Y), to audit DIA's FY 2019 financial statements. E&Y did not issue an opinion because 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 timely provide sufficient evidential support. E&Y 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, E&Y also noted that DIA management's remediation activities were evident and that management continued to enhance efforts to implement process improvements.

Summary of Audit Recommendations[1, 2]

Description	Total Rec	Open Rec	Questioned Costs	Unsupported Costs	Funds to Be Put to Better Use
DIA's Contract Surveillance, 2013-100010-QA	9	1	$500,000	$500,000	-
Indefinite-Delivery/Indefinite-Quantity Contracts, 2016-1004	8	1	-	-	$4,800,000
Government Purchase Card Program, 2016-1006	9	1	-	-	-
Unliquidated Obligations, 2017-1006	19	7	-	-	$250,000,000
Contract Requirements, 2017-1005	4	2	-	-	$4,100,000
Incoming Reimbursable Orders, 2018-1004	2	2	-	-	-
Total	**51**	**14**	**$500,000**	**$500,000**	**$258,900,000**

[1] Financial Statement Audit recommendations are not included.

[2] Management accepted all audit recommendations and is making progress on closing—including the questioned and unsupported costs and funds put to better use.

Summary of Inspection and Evaluation Activity

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

The purpose of the Federal Information Security Modernization Act of 2014 (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.

Inspection and Evaluation Recommendation Summaries[3]

Description	Total Rec	Open Rec	Questioned Costs	Unsupported Costs	Funds to Be Put to Better Use
Defense HUMINT Enterprise, 2017-2006	3	1	-	-	-
Personnel Accountability, 2018-2001	3	1	-	-	-
Personnel Security, 2018-2002	4	2	-	-	-
Supply Chain Risk Management, 2019-2001	7	7	-	-	-
Unauthorized Disclosure, 2019-2006	6	5	-	-	-
Human Capital Services, 2017-2008	3	1	-	-	-
FISMA, 2019-2005	8	8	-	-	-
Total	**34**	**25**	**-**	**-**	**-**

[3] Management accepted all inspection and evaluation recommendations and is making progress on closing.

Summary of Investigative Activity

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.

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 of workplace harassment.

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 of the 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.

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.

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. The total estimated loss to the Government is $88,120.16.

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 2018 to June 2019. We determined a $12,550.19 loss to the Government.

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 by 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 a $8,627.43 loss to the Government.

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.

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 their son's hiring at DIA. 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 benefitted their son's university and a private organization that their son led.

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 senior 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 his 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 2019-7284-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. Management 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 Activities

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[4]	15
Referred to Management (Number of Cases)	15
Referred to Prosecutorial Authority (Number of Cases)	7
Number of Persons Referred to Department of Justice for Criminal Prosecution	1
Number of Persons Referred to State or Local Prosecuting Authorities for Criminal Prosecution (includes military authorities)	0
Total Number of Indictments and Criminal Informations Resulting from Prior Referral to Prosecuting Authorities	1

Investigative Dollars in Reporting Period

Investigation	Number Reprisals	Dollars Identified or Pending Recovery
Time and Labor Fraud	2019-5042-OI	3,154.21
Contractor Cost Mischarging	2019-5045-OI	88,120.16
Time and Labor Fraud	2016-5056-OI	12,550.19
Time and Labor Fraud	2019-5065-OI	8,627.43
Allegations of Unauthorized Receipt of Incentive Pay	2019-7284-WA	40,544.00
Total	**-**	**152,995.99**

Notes

Other Investigative Matters

Description	Quantity
Hotline Program	
DIA OIG Hotline Inquiries Received in Reporting Period	164
DIA OIG Hotline Inquiries Closed in Reporting Period	121
Management Referrals	
Referrals in Reporting Period	8
Referrals in Reporting Period (external agencies)[5]	1

[4] 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.

[5] This case was referred to DoD for further investigation.

Statutory Reporting Summary

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 FY 2018, DIA reassessed its noncompliance with Federal financial management system requirements, and it 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 will be included in the upcoming SAR.

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 SAR.

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. Conference specifics will be outlined in our upcoming SAR.

Summary of 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. Specifics regarding our legislative reviews will be outlined in our upcoming SAR.


DEFENSE INTELLIGENCE AGENCY
UNITED STATES OF AMERICA