

Defense
Intelligence Agency

Office of the
Inspector General

**SEMIANNUAL
REPORT TO CONGRESS**

April 1, 2021–
September 30, 2021



Defense Intelligence Agency Office of the Inspector General

Semiannual Report to Congress 3rd and 4th Quarters, FY 2021

The Defense Intelligence Agency (DIA) Office of the Inspector General (OIG) has strived to make this report as transparent as possible, while safeguarding sensitive information. Where appropriate, we have removed or rephrased information to avoid disclosing classified material. Although we have worked to provide a comprehensive unclassified report, the classified addendum contains additional reports and details that are not publicly releasable.

This report with its classified addendum is posted on the Joint Worldwide Intelligence Communications System and on the Secret Internet Protocol Router Network. A copy of this report, excluding its addendum, 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 OIG at (202) 231-1010.

Send us Your Audit, Inspection, and Evaluation Suggestions

Defense Intelligence Agency
ATTN: Office of the Inspector General
7400 Pentagon
Washington, DC 20301-7400

**Are you aware of the fraud, waste,
or abuse in a DIA
program? If so, report it!**

DIA Inspector General Hotline

Via phone: (202) 231-1000

Via NIPR email: ig_hotline@dia.mil

Contents

General Information

- 01 The DIA Office of the Inspector General
- 02 Message from the IG
- 03 DIA OIG Organization
- 05 Whistleblower Protections

Reporting

- 06 Statutory Reporting
- 08 Legislative and Regulatory Review
- 09 Conference Reporting
- 10 Summaries of Audits Division Activity
- 12 Summaries of Inspections and Evaluations
Division Activity
- 16 Summaries of Investigations Division Activity
- 24 Appendix A: Statistical Tables
- 32 Appendix B: Status of Recommendations
- 47 Appendix C: Audits, Inspections, Evaluations,
and Investigations closed since April 1, 2021
- 51 Appendix D: Index of Reporting Requirements

The DIA Office of the Inspector General

The Defense Intelligence Agency (DIA) Office of the Inspector General (OIG) is one of 75 Federal statutory Inspectors General (IGs) established by the IG Act of 1978, as amended. The IG Act requires OIG independence and objectivity, and contains safeguards against efforts to impair or hinder OIG operations.

Our Mission

Conduct independent, objective, and timely oversight across the DIA Enterprise to promote economy; deter and detect fraud, waste, abuse, and mismanagement; and inform DIA and Congress. We accomplish this through independent audits, inspections, evaluations, investigation, and the OIG Hotline Program.

Our 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.



Our Values

Teamwork

Partner internally and across organizational boundaries to achieve common goals.

Excellence

Provide high quality customer service and value-added products.

Accountability

Deliver timely solutions that assign responsibility and meet the highest standards.

Initiative

Apply insight and agility to solve challenges and organize priorities.

Integrity

Apply insight and agility to solve challenges and organize priorities.

A Message from the IG

Kristi M. Waschull

Dedicated, innovative, and motivated—these are the sort of words that come to mind when I think about the women and men who worked in the Defense Intelligence Agency (DIA) Office of the Inspector General (OIG) during the last six months. This Semiannual Report to Congress presents the results, findings, and statuses of my team’s audits, inspections, evaluations, and investigations from April 1, 2021, to September 30, 2021.

The reconstitution from the impacts of the 2019 Coronavirus pandemic during this period was a unique experience. My staff rose to the challenge and was an Agency leader in receiving the vaccine, demonstrating their professionalism, and commitment to their work. Their dedication allowed OIG to continue to conduct relevant and timely oversight to detect and deter fraud, waste, and abuse, and help DIA address identified management challenges and achieve the desired end state in the Director’s 2021 DIA Strategy.

OIG efforts continue to focus on strategic issues facing the Agency. Work completed by both our Audits and Inspections and Evaluations Divisions addressed 2020 Top Management Challenges, including Financial Management, Information Security Governance, and Leadership Controls and Oversight. In addition, the evaluation of DIA’s Foreign Disclosure Program and the Fiscal Year 2021 Report on Classification both contributed to advancing the Allies and Partnerships line of effort in the Director’s 2021 DIA Strategy.

The Investigations Division continued its work investigating allegations of fraud, waste, reprisal, and abuses of authority; our Hotline branch screened thousands of communications, responding when appropriate and referred cases to our Investigations Division or Agency management for action. In this reporting period, we saw our investigative efforts result in a Federal District Court Conviction with a contract employee ordered to make restitution of over \$107,000 and sentenced to confinement for over a year. Also, at our request, the Agency swiftly debarred the contract employee from further Federal contracts. Efforts by the investigators help strengthen integrity, accountability, and transparency, which lead to strengthening Agency leadership controls and oversight, again a persistent top management challenge.

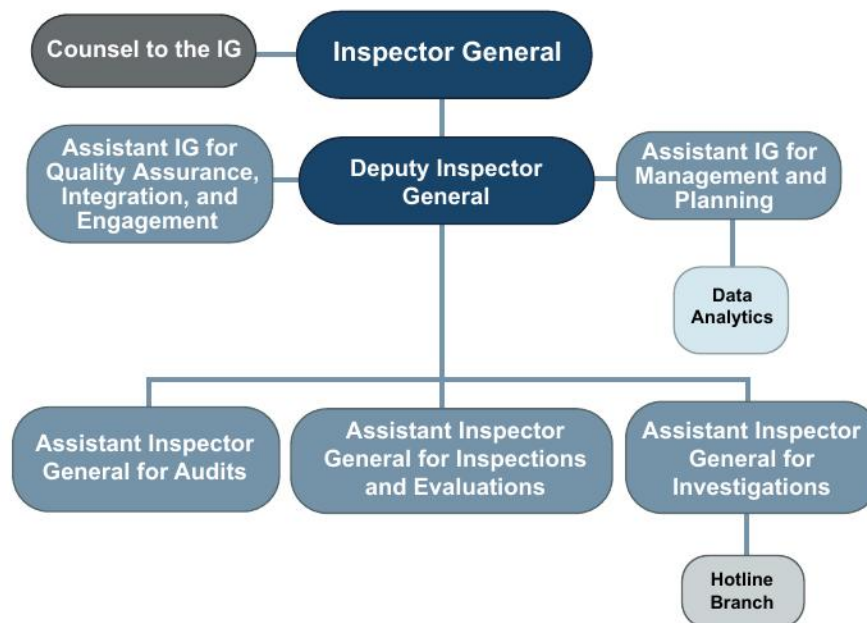
As the Agency adjusts to the “new normal,” OIG’s ability to perform our mission in an effective and timely manner remains dependent on the collaborative efforts between my staff and Agency management to address OIG findings and to implement the recommended corrective actions. I would like to express my appreciation to DIA leadership for the sustained commitment to supporting our important work. The Director’s Agency-wide message highlighting the requirement to cooperate with OIG demonstrated this commitment.

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 through <http://www.dia.mil/About/Office-of-the-Inspector-General/> and <http://www.oversight.gov>.



Kristi M. Waschull
Inspector General

OIG Organizational Chart



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 oversees the annual independent audit of the Agency’s financial statements.

Inspections and Evaluations

The Inspections and Evaluations Division inspects and evaluates 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 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 and the Information Management & Compliance Office (IMO), also reports and investigates questionable intelligence activities, as defined by Executive Order 12333, “United States Intelligence

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 program’s primary role is to receive and evaluate concerns and complaints and determine the Agency element best suited to take appropriate action.

Management and Planning

The Management and Planning Division manages all administrative programs and services directly supporting OIG. The Division enables audit, inspection, evaluation, and investigation activities and facilitates timely production of intelligence management and oversight products for DIA senior leadership and congressional overseers. Management and Planning Division functions include, but are not limited to: 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.



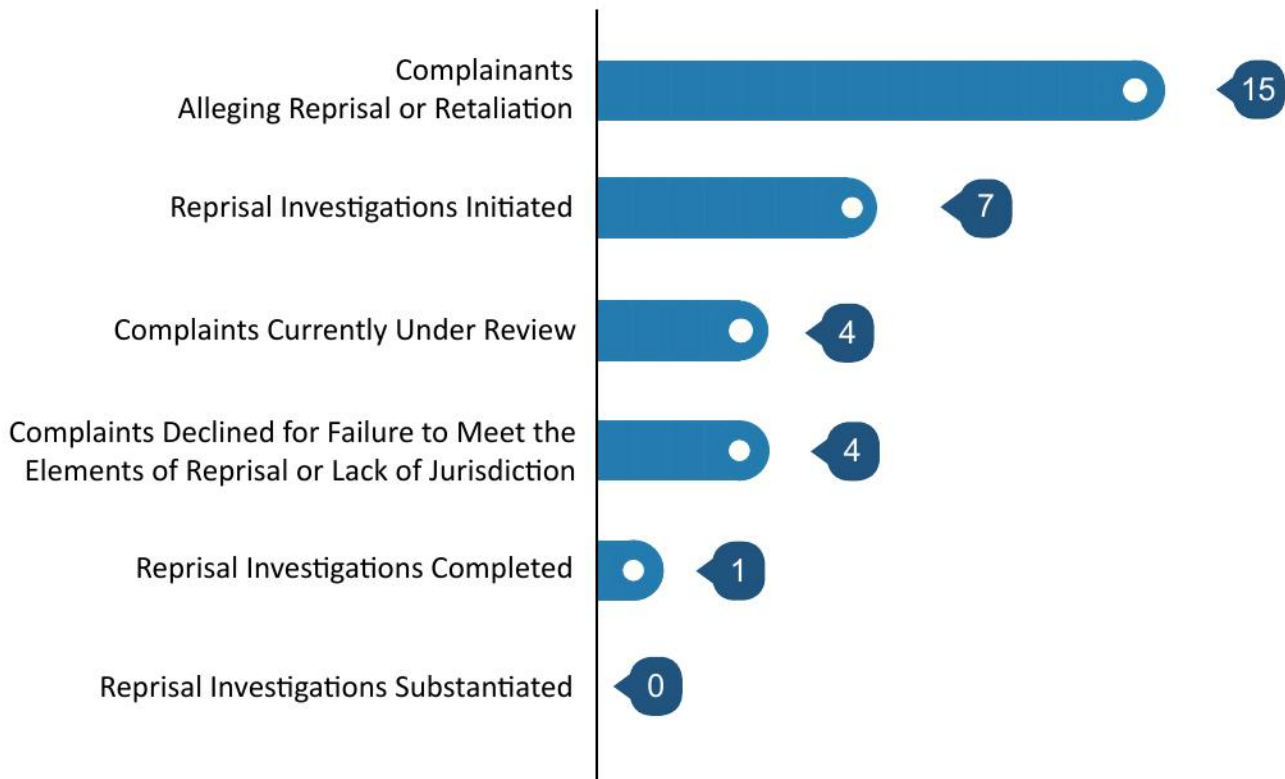
“It is through our diligent work and steadfast spirit that our organization continues to compel management action and keep Congress fully and currently informed.”

Kristi M. Waschull,
Inspector General

Whistleblower Protections

Protecting whistleblowers is vitally important to us and so is educating DIA personnel about their duty to report wrongdoing and the protections afforded to whistleblowers—those who in good faith report fraud, waste, abuse, and other wrongdoing to us and other authorized entities. Our office has expanded its reporting concerning whistleblower trends as we continue to investigate allegations of reprisal or retaliation against whistleblowers. We aim to advise whistleblowers of the results of these investigations, and to issue reports with recommendations for corrective action to make whistleblowers, who have been retaliated or reprimed against whole, and to recommend the Agency take appropriate disciplinary action against offenders. Our personnel work rigorously to preserve the confidentiality of individuals who provide us with information, unless those individuals consent to disclosure or disclosure is determined to be unavoidable during the course of an investigation. Reports of investigation are written with a view towards protecting the anonymity of witnesses—consistent with due process and privacy policies.

We also participate in Agency training seminars for supervisors and senior leadership on whistleblower protections and issue monthly bulletins on the same topic. On National Whistleblower Appreciation Day in July, and again in August, we issued Agency-wide bulletins reminding employees, service members, and contractors of their duty to report and the protections from reprisal and retaliation afforded whistleblowers. During this reporting period, we received fifteen complaints alleging reprisal or retaliation¹:



¹ We log reprisal complaints when we receive and review them to determine if an investigation will be initiated. When investigative activity is complete, we ordinarily find that allegations of reprisal or retaliation are substantiated or unsubstantiated. We advise Whistleblowers that they may request further review of our findings by the Intelligence Community IG or DoD IG.

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 the 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.

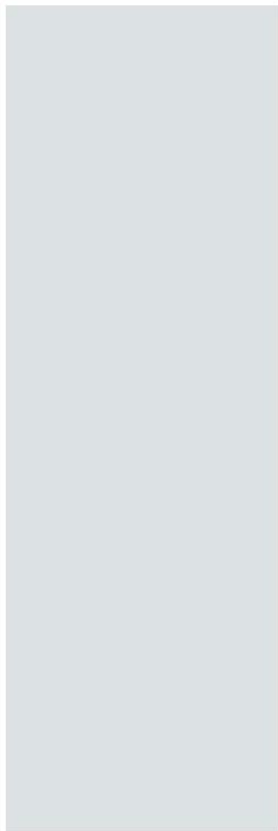
Federal Financial Management Improvement Act of 1996

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.

Statutory Reporting Cont'd

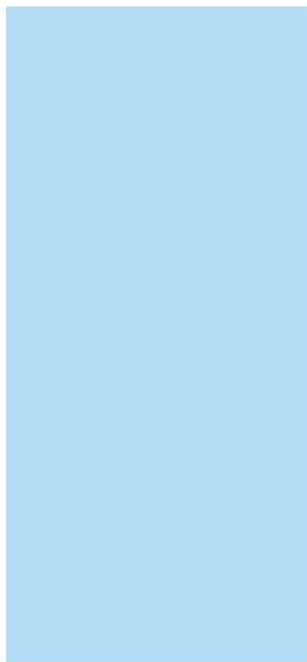
Attempts to Interfere With the IG's Independence

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. During this period, there were no noted instances involving interference with the IG's independence.



Public Disclosure

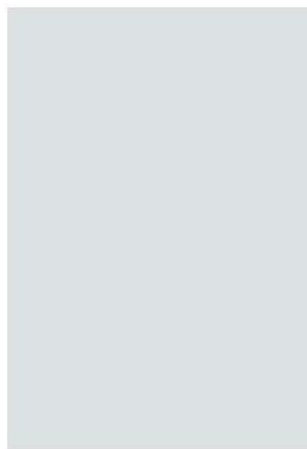
Section 5(a)(22) of the IG Act of 1978, as amended by the IG Empowerment Act, requires IGs to provide detailed descriptions of inspections, evaluations, audits, and investigations involving senior Government employees that were closed during the reporting period without being publicly disclosed. Summaries of all such work are included in the appropriate sections of this report.



Peer Reviews

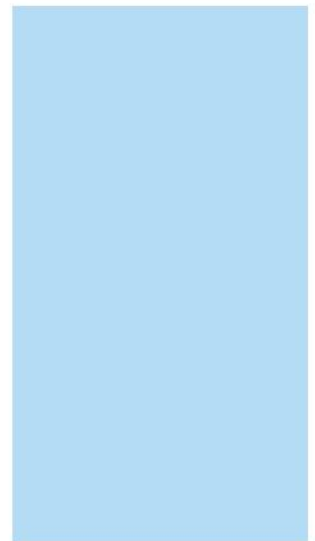
Sections 5(a)(14–16) of the IG Act require IGs to report information about peer reviews that their offices have been subject to, including any recommendations that have not been fully implemented and a justification as to why.

On January 22, 2021, the National Geospatial-Intelligence Agency OIG completed a peer review of our Audits covering the preceding 3 years. They issued a pass rating and all recommendations have been implemented. Also, 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.



National Defense Authorization Act of Fiscal Year (FY) 2020

Section 6718(b) of the FY 2020 National Defense Authorization Act 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.



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. We review legislation, executive orders, DoD and Agency policy, 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:

22	Legislation
11	Department of Defense Issuances
10	Defense Intelligence Agency Issuances
1	Office of the Director of National Intelligence Issuances
1	Executive Orders

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. We have also not verified whether DIA employees hosted or attended these conferences—either in person or virtually—in light of the Coronavirus (COVID-19) pandemic.

Conference Name	Type	Estimated Cost	Actual Cost
Indo-Pacific Intelligence Chiefs Conference 2021	DIA Jointly-Hosted	\$388,715.00	\$282,042.00
2nd Annual DoD IG Underground Domain Symposium	DIA Jointly-Hosted	\$81,602.00	Pending
2021 Department of Defense Intelligence Information System Worldwide Conference	DIA Hosted	\$817,100.00	Pending
Society for Human Resources Management FY 2021 Conference	Non-DoD Hosted	\$32,646.00	Pending
42nd Annual Blacks in Government	Non-DoD Hosted	\$34,336.00	Pending
FY 2021 Joint Reserve Intelligence Program Annual Conference	DIA Hosted	\$255,790.00	\$230,925.84



Summary of Audits Division Activity

Evaluation of DIA's Information Security Continuous Monitoring Program, Project 2021-1001

We evaluated DIA's Information Security Continuous Monitoring Program as part of a joint project across the IC. The intent of the project was to identify common causes within the IC for longstanding observations from the Federal Information Security Modernization Act review conducted over the prior years. Management agreed with our recommendation. For more information on the project and results, please see the "Classified Summaries of Audits Division Activity" section in the Classified Addendum.

Evaluation of DIA's Compliance with the Improper Payments Elimination and Recovery Act for Fiscal Year 2020, Project 2021-1005

We evaluated DIA's compliance with the Improper Payments Elimination and Recovery Act (IPERA) for FY 2020. IPERA requires each Federal agency to report improper payments in its Agency Financial Report (AFR) and assess risks once every 3 years for susceptible programs. We determined the Agency reported improper payments in its annual AFR, but also identified that the Agency did not perform a risk assessment for all improper payment programs. This occurred because DIA management relied on a risk assessment for the Managers' Internal Control Program (MICP) to satisfy IPERA requirements. Project results aligned with our DIA FY 2020 Top Management Challenge—Financial Management. Management agreed with our recommendation.

Other Audits Division Activity

We issued two recommendations this reporting period. We also closed 11 of the 28 recommendations that remained open at the end of the previous reporting period. We continued to coordinate with Agency management on the status of its corrective action plans for the remaining open recommendations.

Summary of Ongoing Audits Division Activity

Audit of Emergency and Extraordinary Expenses, Project 2020-1001

Our objective for this audit is to determine whether DIA's Emergency and Extraordinary Expenses are properly authorized and the reimbursement is properly supported. Project results will help the Agency address our DIA FY 2020 Top Management Challenge—Financial Management. We were in the planning phase by the end of the reporting period.

Audit of DIA's Fiscal Year 2021 Financial Statements, Project 2021-1004

Our objective for this audit is to determine the reliability of data and reasonableness of DIA's financial statements. We are also examining disclosures in accordance with applicable guidance and reviewing the reliability of financial systems, effectiveness of internal controls, and compliance with laws and regulations. Project results will help the Agency address our FY 2020 Top Management Challenge—Financial Management. We were in the fieldwork phase by the end of the reporting period.

Audit of DIA's Machine-assisted Analytical Rapid-repository System Program, Project 2021-1006

Our objective for this audit is to determine whether DIA's Emergency and Extraordinary Expenses are properly authorized and the reimbursement is properly supported. Project results will help the Agency address our DIA FY 2020 Top Management Challenge—Financial Management. We were in the planning phase by the end of the reporting period.

Evaluation of DIA's Government Travel Charge Card, Project 2021-1007

Our objective for this evaluation is to determine whether DIA's Government Travel Charge Card reimbursements are appropriate and timely. Project results will help the Agency address our DIA FY 2020 Top Management Challenge—Financial Management. We were in the reporting phase by the end of the reporting period.

Evaluation of DIA's Compliance with the Federal Information Security Modernization Act, Project 2021-1008

Our objective for this evaluation is to determine whether DIA's overall Information System Security Program is effective. Project results will help the Agency address our DIA FY 2020 Top Management Challenge—Information Security Governance. We were in the reporting phase by the end of the reporting period.



Summary of Inspections and Evaluations Division Activity

Fiscal Year 2021 Report on Classification, Project 2021-2002

We evaluated the accuracy of the application of classification and handling markers on a representative sample of DIA's finished reports. We also evaluated DIA's compliance with declassification procedures and the effectiveness of DIA's processes for identifying topics of public or historical importance that merit prioritization for a declassification review. We determined that DIA did not consistently apply accurate classification and handling markers to finished intelligence reports because it lacked a uniform, corporate approach to ensure classification accuracy. Additionally, we determined that DIA made limited progress toward meeting Federal and DoD requirements to declassify Agency records because it did not prioritize the development, operation, or scalability of its declassification program. These issues impacted DIA's information sharing priorities and limited transparency with legislative, diplomatic, and public stakeholders. Project results aligned with our DIA FY 2020 Top Management Challenge—Information Security Governance. Management agreed with all seven of our recommendations.

Evaluation of DIA's Foreign Disclosure Program, Project 2019-2008

We evaluated the Agency's implementation of IC and DoD policies, and Agency processes and practices, for disclosing classified military intelligence. We found that DIA's Foreign Disclosure Program was not positioned to effectively manage foreign disclosure activities and ensure adherence to governing policies. We determined gaps existed within foreign disclosure program management, oversight, information management, and strategic human capital planning, creating additional risk to the Foreign Disclosure Program and disclosure processes. Project results aligned with our DIA FY 2020 Top Management Challenge—Leadership Controls and Oversight. Management agreed with all three of our recommendations.

Management Alert on Service Element Pay and Support for Personnel Assigned to the Defense Attaché Service, 2021-2005

We completed a research project on the Defense Attaché Service (DAS) in response to concerns brought to our attention about leadership, culture, and management. The research project was designed to identify areas most in need of our attention for a 90-day follow-on evaluation. On September 14, 2021, we initiated our follow-on evaluation of the Defense Attaché Training. However, through our research we also learned that service members assigned to Defense Attaché Offices experienced systemic delays and disruptions to essential administrative actions. This caused an undue burden to some service members and negatively influenced their morale. As a result, we issued a management alert related to service element pay and support for personnel assigned to the DAS, and we requested that the Agency provide corrective actions or a plan of action to address the identified issues.

Peer Review of the National Geospatial Agency Office of the Inspector General Inspection and Evaluation Organization

We led an IC OIG External Peer Review of the National Geospatial-Intelligence Agency (NGA) OIG Inspection and Evaluation Organization, covering reports issued between April 1, 2018, and March 31, 2021. The peer review was accomplished in accordance with the Council of Inspectors General on Integrity and Efficiency (CIGIE), “Guide for Conducting External Peer Reviews of Inspection and Evaluation Organizations of Federal Office of Inspector General,” December 2020. The cross-IC team determined the NGA OIG Inspection and Evaluation Organization’s internal policies and procedures generally were consistent with the seven CIGIE Blue Book standards addressed in the external peer review. Of the four reports reviewed, four reports, generally complied with the seven covered CIGIE Blue Book standards.

Other Inspection and Evaluation Activity

We issued 11 new recommendations and engaged with DIA management on their progress to implement the 33 open recommendations issued in prior reporting periods. We did not close any recommendations this reporting period.

We participated in a separate peer review, Central Intelligence Agency OIG’s Inspection and Evaluation Organization, covering reports issued between April 1, 2018, and March 31, 2021. The peer review was also accomplished in accordance with CIGIE, “Guide for Conducting External Peer Reviews of Inspection and Evaluation Organizations of Federal Office of Inspector General,” December 2020.

Summary of Ongoing Inspections and Evaluations Division Activity

Evaluation of DIA's Management of Reserve Military Intelligence Capabilities, 2020-2005

Our objective for this evaluation is to assess DIA's management of the DoD Joint Reserve Intelligence Program across the Defense Intelligence Enterprise. We are also assessing DIA's administration and use of reserve military intelligence capabilities to meet mission requirements throughout DIA. Project results will help the Agency address our DIA Top Management Challenge—Leadership Controls and Oversight and DIA Emerging Risk—Human Capital and Talent Management. We issued our draft report and were awaiting management response by the end of the reporting period.

Study of DIA's Response to the COVID-19 Pandemic and Impacts to Critical Mission Functions and Strategic Priorities, Project 2021-2001

We initiated this study in October 2020 due to interest from Congressional stakeholders and Agency leadership to report on COVID-19 impacts to DIA critical missions, information security, and workforce health and safety. We obtained and reviewed select data from Agency elements for calendar years 2018–2020 to identify mission impacts from COVID-19 and to capture the information for historical reference and potential future review. However, due to the wide scope of this study and competing priorities, we determined it would not be feasible to complete the study at this time. In spite of this decision, we did review all of the information obtained during the course of the study and we will outline several observations for the Agency's consideration. The information gathered during this study also helped inform and reinforce conclusions from other oversight work to identify Contingency Planning as an Agency top management challenge. We were drafting a closure memorandum at the end of the reporting period.

Evaluation of Analytic Talent Management, Project 2021-2003

Our objective for this evaluation is to evaluate the effectiveness of DIA's recruitment, hiring, placement, and retention of officers in the analysis career field. Project results will help the Agency address our DIA Emerging Risk—Human Capital and Talent Management. The project was paused in the planning phase, due to other project priorities, by the end of the reporting period.

Evaluation of DIA's Management of the Open Source Intelligence Integration Center, 2021-2004

Our objectives for this evaluation are to determine the effectiveness of the Open Source Intelligence (OSINT) Integration Center's support to DIA and the effectiveness of DIA's management of OSINT for the Defense Intelligence Enterprise. Project results will help the Agency address our DIA Top Management Challenge—Information Security Governance. The evaluation was in the planning phase by the end of the reporting period.

Evaluation of the Defense Attaché Training Program, Project 2021-2005

We initiated this 90-day evaluation as a result of our 30-day DAS research project, initiated in response to concerns brought to our attention about leadership, culture, and management, and designed to inform the follow-on evaluation focus. Our objective for this evaluation is to evaluate development, governance, and oversight of DAS training programs. Project results will help the Agency address our DIA Top Management Challenge—Leadership Controls and Oversight. The evaluation was in the fieldwork phase by the end of the reporting period.



Summary of Investigations Division Activity

Investigative Activity Oversight

Reprisal Investigations

We completed one investigation involving allegations of reprisal and abuse of authority made during the previous reporting period. We did not substantiate the allegations in this case.

During this reporting period, we received 15 reprisal complaints (14 from DIA personnel and one referral from the Department of Defense Office of the Inspector General [DoD IG]):

- Seven of the complaints are under active investigation by our office,
- Three complaints did not meet the *prima facie* elements of reprisal,
- One complaint, which was referred from the DoD IG, was determined to have no nexus to DIA (including Agency-related personnel),
- The remaining four complaints are presently under review.

When we determined that the aforementioned reprisal complaints did not meet the *prima facie* elements of reprisal, we notified the employees in writing of our determination and of the employees right to an external review by the IC IG or in some instances the DoD IG. We also provided copies of the notifications to the DoD IG and IC IG for their awareness in case the employees sought external review of our determination.

Summaries of Published Investigative Reports

Travel Fraud and Misuse of Emergency and Extraordinary Expense Funds Investigation, Case 2019-005012-01

We substantiated allegations of travel fraud and misuse of Emergency and Extraordinary Expense funds made against a former DIA senior enlisted member. Specifically, we determined that the former enlisted member violated three articles of the Uniformed Code of Military Justice (UCMJ) when they prepared, signed, and submitted a fraudulent travel request and subsequent travel voucher for travel to Washington, DC, for one week. As a result, we estimated a total loss to the Government of \$4,475.14.

During the same incident, we also determined the former senior enlisted member and a DIA civilian employee violated guidance from a Chairman of the Joint Chiefs of Staff Instruction (CJCSI) by sharing user identification and password information in order to access the Department of State electronic travel application. Although we did substantiate violation of UCMJ, we did not substantiate any violation of Federal criminal law; therefore, this case was not referred to the appropriate Assistant United States Attorney (AUSA) for consideration of criminal prosecution.

In addition, our investigation cited four management deficiencies that, if addressed, could have precluded or at least mitigated the unauthorized actions by the former enlisted member. All recommendations, disciplinary actions, and recovery of funds are pending further action by the Agency.

Violation of Agency Policy Investigation, Case 2020-005013-01

We did not substantiate allegations against a DIA civilian employee for violating U.S. Army War College (USAWC) policy and displaying poor academic professionalism by publishing an article in the Military Review journal using incomplete USAWC research without review before publication. We determined that there was insufficient evidence to substantiate if the employee violated any law, regulation, or policy when they used USAWC's research. We also determined that the employee failed to follow DIA policy when they prepared and submitted a separate, inaccurate prepublication request to DIA leadership for a different publication. Disciplinary action is pending further action by the Agency.

Contractor Cost Mischarging Investigation, Case 2020-005027-01

We substantiated allegations of false official statements, false claims, and theft of public funds against four DIA contractor employees. Following initial notification from a DIA contracted commercial firm, we determined that between February 25, 2019, and March 11, 2021, four contractor employees, working for two separate companies, had collectively prepared and submitted fraudulent timesheets claiming a total of approximately 852.49 hours they did not work. The total loss to the Government was estimated at \$78,585.31. Since these activities represented a violation of law, we referred this case to the appropriate AUSA, who declined criminal prosecution. DIA management subsequently recovered, from the first of the two contractor companies, \$44,893.05, and also received an additional cost avoidance of \$12,030.00. DIA management is presently working with the second contractor company to recover the loss of \$21,662.26. DIA management is presently determining if suspension or debarment actions are warranted (i.e., under Subpart G—Suspension, 2 Code of Federal Regulations (C.F.R.) § 180.800 and Subpart H—Debarment, 2 C.F.R. § 180.800) against any of the four contractor employees.

Reprisal & Abuse of Authority Investigation, Case 2021-000004-01

We did not substantiate various allegations—including reprisal and abuse of authority—made by a military officer (formerly assigned to DAS) against two DIA supervisory civilian employees and two DIA supervisory military officers, also assigned to DAS. The Complainant alleged that, after having made earlier protected communications, one of the two supervisory civilian employees reprised against the Complainant by eliminating them from consideration for future assignment with DIA. Further, the Complainant alleged that one of the two supervisory military officers reprised against the Complainant, after having made earlier protected communication, by changing the Complainant’s performance evaluation rater to the other military officer and receiving a perceived subpar annual evaluation. The Complainant also alleged that the two supervisory civilian employees committed fraud, waste, and abuse by traveling overseas for reasons besides their official purpose.

We determined that the supervisory civilian employee acted within their authority when they considered the Complainant for future assignment. We did not substantiate additional allegations of Reprisal involving the change of military performance evaluation rater, which was done in accordance with both DIA and military service policies. Finally, we also determined there was insufficient evidence to substantiate the Complainant’s other allegations—to include obstruction of justice, witness intimidation, gross mismanagement, and fraud, waste, and abuse—against any of the four subjects identified earlier. We did not substantiate any violation of Federal criminal law; therefore, this case was not referred to the appropriate AUSA for consideration of criminal prosecution.

Misuse of Government Travel Credit Card Investigation, Case 2021-000010-OI

We substantiated allegations of misuse of a Government Travel Credit Card (GTCC) by a DIA employee. Specifically, we determined that the employee violated DoD guidance, when they made and subsequently paid for numerous personal transactions and cash withdrawals using their GTCC while on travel between January 2019 and May 2020, amounting to \$14,395.05. There was insufficient evidence to support a criminal referral to an AUSA; however, disciplinary action for violating GTCC regulations is pending by the Agency.

Abuse of Authority, Hostile Work Environment, and Mishandling Personal Identifying Information and Personal Health Information Investigation, Case 2021-000018-OI

We did not substantiate allegations made against two DIA civilian senior officials (one of who is now retired) for abusing their authority, creating a hostile (office) work environment, or for mishandling DIA employee's sensitive personal identifying information (PII) and personal health information (PHI). However, we did determine that two Agency military staff officers violated DIA Directive [DIAD] 5400.500, "Privacy and Civil Liberties Program," November 9, 2020, when they breached Agency systems and repeatedly gained access to employee PII/PHI. We also determined that the officers violated article 92, Uniform Code of Military Justice, "Failure to Obey Order or Regulation," undated, when they continued to access the PII and PHI data after being told by DIA senior leadership that they were prohibited from accessing, reviewing, or maintaining the information. Our case was referred to the appropriate general court-martial convening authority for appropriate administrative or criminal action under the UCMJ. Disciplinary action is pending.

During the course of the investigation, we notified the Director, DIA, of the breach of PII and PHI, and the failure of Agency personnel to report the breach. We also informed the Director that IMO reported they filed a PII breach notice to the DoD Privacy Office; the Office of Human Resources reported they have been clarifying appropriate use of data; and the Chief Information Office (CIO) reported they started setting controls with data owners to lockdown or remove data. We strongly stressed to the Director the importance of DIA safeguarding and protecting PII/PHI data across the Enterprise. After publishing the report, we requested the Agency verify that the aforementioned actions were completed and to determine whether notification to affected Agency employees, that their personal information may have been compromised, is warranted.

Time and Labor Fraud Investigation, Case 2020-005016-OI

We substantiated allegations of time and labor fraud, false official statements, false claims, and theft of public funds by a DIA employee. The employee fraudulently prepared, signed, and submitted timesheets from December 23, 2018, to December 21, 2019, totaling 308 regular work hours that they did not work. We estimated a \$17,144.73 loss to the Government. Since this represented a violation of law, we referred this case to the appropriate AUSA, who declined criminal prosecution. Disciplinary action and recoupment of funds are pending by the Agency.

Significant Management Referrals²

Conduct Unbecoming, Case 2020-005042-WA

We received a complaint from a non-DIA civilian that a U.S. Air Force (USAF) reserve officer, formerly assigned to DIA, tried to maintain an adulterous relationship with the Complainant's spouse through repeated attempts to text and phone individuals in the Complainant's household. As such, we referred this matter to Agency management for further inquiry. However, Agency management subsequently discovered that the reserve officer had already retired from military service prior to the original filing of subject complaint and, as such, fell outside of Agency management authority.

Mishandling of Analytical Production, Case 2021-000015-WA

We received an anonymous complaint alleging an element in DIA produced analytical assessments that contained uncorroborated evidence as part of its analytic production. However, the complaint failed to provide us with any further specific information relevant to when or how this uncorroborated evidence was allegedly used. Despite the lack of substance in the allegation, we considered the potential risk of such and referred the matter to Agency management for review, inquiry and action as deemed appropriate. Agency management subsequently, independently reviewed and reaffirmed their analytic methods and standards used in its production of the referenced products.

Security Matter, Case 2021-000023-WA

We were notified by the U.S. Transportation Command (USTRANSCOM) OIG of a security matter involving the improper retention and storage of unclassified information technology (IT) equipment in a USTRANSCOM secure facility. Upon request, USTRANSCOM provided us with a copy of their report of inquiry into the matter. Since the allegation involved the reported improper retention and storage associated with a secure facility, which is a security matter, we referred the matter to Agency management for further inquiry and action as deemed appropriate. Action by Agency management is pending.

Failure to Follow Prescribed Operating Procedures, Case 2021-000025-WA

We received a complaint alleging that several DIA directorates, offices, and programs failed to follow prescribed Agency operating procedures with regard to reporting and addressing sexual assault complaints made by DIA employees when DIA was conducting limited on-site, office operations due to the COVID-19 pandemic. Specifically, the Complainant alleged that due to their particular classified employment status and the multiple incidents and miscommunications in DIA's "hybrid" work environment, the Complainant endured undue personal hardship due to the significant delays by Agency elements to provide appropriate victim services. We were informed by the Agency that they investigated the underlying sexual misconduct, initiated action against the senior official, and have begun to take corrective action. Further action by Agency management regarding their failure to provide appropriate services to Agency employees in a classified employment status is pending.

Policy Matter, Case 2021-000026-WA

We received an anonymous complaint that DIA failed to follow DoD guidance as it relates to DIA's personnel security program. Specifically, the Complainant alleged that DIA has been implementing a fitness process for civilian applicants for over 3 years without published policy by the Director, DIA. Since this matter involves an alleged lack of policy for fitness and suitability determinations, we determined that this matter was more suited for review, inquiry, and action by Agency management as deemed appropriate. Action by Agency management is pending.

Security Matter, Case 2021-000027-WA

We received a complaint (referred from the DoD OIG) alleging that a DIA employee stored classified information on a personal computer at their residence. Since the allegation involved the improper retention and storage of classified information, we referred the matter to Agency management for further inquiry and action it deemed appropriate. Agency management is conducting an inquiry into the allegation.

Policy Matter, Case 2021-000028-WA

We received a complaint alleging that select DIA senior leadership violated Office of Personnel Management (OPM) and Agency policies with regard to implementing operating status, specifically regarding operations during inclement weather and operations with regard to telework. The Complainant also alleged that select DIA senior leadership had violated Agency policy by improperly reorganizing the structure of subordinate offices. We determined that select DIA senior leadership may have the appropriate authority to execute these identified management decisions, but it is unknown if they followed appropriate Agency policies to implement those decisions. Therefore, we referred this matter to DIA leadership to review and determine whether the management decisions were in accordance with OPM and Agency policy. Agency management has appointed an inquiry officer to conduct an inquiry into the allegations.

Improper Disposal of Government Property, Case 2021-000029-WA

We received a complaint alleging that two television sets, purchased earlier by DIA, had been improperly disposed of by Agency personnel. Since the allegation involved the improper disposal of Government property, we determined that DIA management would be better suited to review this complaint and further inquire into the matter. Therefore, we referred this matter to DIA management for review and further inquiry. Currently, Agency management is conducting an administrative inquiry into the allegation, and final action is pending.

Firearms Policy, Case 2021-000037-WA

We received an anonymous complaint alleging that a DIA employee was identified by several employees for carrying a firearm on Federal property without the proper identification or appropriate authority. We determined the complaint fell within the purview of Agency management for further inquiry and action as deemed appropriate. Action by Agency management is pending.

Violation of Agency COVID-19 Guidance, Case 2021-000040-WA

We received a complaint alleging that an Agency office had posted information on their online, classified website identifying DIA employees (by name) and their COVID-19 vaccination status. We referred the matter to the Agency office cited in the complaint for further inquiry and action as deemed appropriate. The office subsequently confirmed that all related information had been removed from the office's website and that complete examination of the website confirmed no other such information is available. The office also coordinated the matter with IMO to confirm that appropriate actions had been taken. They also worked with IMO to obtain Privacy Act advisory information and information on how to handle Agency COVID-19 data, which was shared with office leadership.

Misuse of Government Resources

We received 10 separate complaints citing various respective misuses of Government resources by Agency personnel (i.e., 1 DIA civilian employee, 1 DIA enlisted military member, and 8 DIA contractor employees). Using Agency equipment and Government unclassified internet access, these individuals conducted a variety of unauthorized activities, including searching through a variety of websites containing explicit content, accessing and viewing a variety of unauthorized materials containing inappropriate content, and conducting sexually explicit internet message exchanges. In each of these cases, we referred the matter to Agency management for further inquiry and action as deemed appropriate. Action by Agency management is pending in each of these cases.

Due to the increase in unauthorized activity, on September 14, 2021, CIO issued an advisory to the entire DIA workforce (including contractor employees) reminding them of their roles and responsibilities when accessing DIA IT systems.

Coronavirus Related Complaints and Management Referrals

Due to the critical importance of workforce safety and mission, we have kept management aware of COVID-19 related complaints. During this reporting period, we received 28 COVID-19 related complaints. Of the 28 complaints, 15 were allegations of non-compliance, 7 were requests for information, and 3 were allegations related to workforce reconstitution concerns. The remaining three complaints did not involve the aforementioned allegations but did reflect COVID-19 concerns. Overall, we closed 21 complaints and opened 1 investigation. We are currently reviewing the remaining six complaints.

Investigative Activity Support

Personnel Vetting

We completed 3,235 checks for derogatory information within OIG records in response to 283 requests, originating 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, Inspection, and Evaluation Reports and Recommendations with Questioned and Unsupported Costs

Description	Number of Reports	Questioned Costs	Unsupported Costs
No management decision was made by March 31, 2021 ³	1	\$1,500,000	\$1,500,000
Issued during this reporting period	–	–	–
Costs disallowed by management	–	–	–
Costs allowed by management	1	\$1,500,000	\$1,500,000
No management decision was made by September 30, 2021	0	-	-

³ Evaluation of DIA’s Implementation of CARES Act—section 3610, Project 2020-1006, was published in DIA OIG Semiannual Report to Congress (October 1, 2020–March 31, 2021). We found that for all 17 CARES Act-related reimbursements we reviewed, totaling \$1.5 million, DIA could not show that the reimbursements were appropriate. Management agreed with the corresponding recommendations.

Table A-2: Audit, Inspection and Evaluation Reports with Recommendations that Funds be Put to Better Use

Description	Report Number	Funds to be Put to Better Use
No management decision was made by March 31, 2021 ⁴⁵⁶	3	\$250,614,000
Issued during this reporting period	–	–
Dollar value of recommendations not agreed to by management ⁷	1	\$250,000,000
No management decision was made by September 30, 2021	–	–
No management decision was made by September 30, 2021 ⁸	2	\$614,000

⁴ Audit of DIA’s Unliquidated Obligations, Project 2017-1006, was 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, despite obligating nearly all funds. Management has closed six of the recommendations and is working on the last open recommendation.

⁵ Audit of Information Technology Services Contracts, Project 2018-1006, was published in DIA OIG Semiannual Report to Congress (April 1, 2020–September 30, 2020). We found that more than \$438,000 in award fee payments could have been used for other mission requirements. Management has not closed the recommendation.

⁶ Audit of Unplanned Price Changes, Project 2019-1006, was published in DIA OIG Semiannual Report to Congress (October 1, 2020–March 31, 2021). We found that DIA could have saved \$176,000 for other mission priorities if it had analyzed and negotiated price escalation for option periods using data maintained by the Bureau of Labor Statistics.

⁷ (During this period, DIA management closed the last recommendation for the Audit of DIA’s Unliquidated Obligations, Project 2017-1006.

⁸ \$614,000 of the \$250,614,000 for which no management decision was made by March 31, 2021, was overdue by 6 months or more.

Table A-3: Investigations Dollar Recoveries in Reporting Period

Investigation	Report Number	Effective Recovery Date	Dollars Recovered
Contractor Cost Mischarging	2020-005027-01	Mar 3, 2020	\$ 44,893.05 (partial recovery)

Table A-4: Investigative Activities⁹

Description	Quantity
Cases Opened in Reporting Period	51
Cases Closed in Reporting Period	4
Cases Still Open at End of Reporting Period ¹⁰	93
Investigation Reports Issued in Reporting Period ¹¹	7
Management Referrals in Reporting Period ¹² (Number of Cases)	24
<ul style="list-style-type: none"> • Referred to Agency Management (Number of Cases) 	31
<ul style="list-style-type: none"> • Referrals resulting from Reports of Investigation in Reporting Period¹³ 	7
Referrals resulting from direct referral of evaluated complaints ¹⁴	24
Referred to Prosecutorial Authority (Number of Cases)	2
Number of Persons Referred to State or Local Prosecuting Authorities for Criminal Prosecution (includes military authorities)	0
Total Number of Indictments and Criminal Prosecution Resulting from Prior Referral to Prosecuting Authorities	1

⁹ Description of Metrics: All metrics provided were developed as a result of reviewing all relevant individual cases, including those opened and closed during the reporting period and cases remaining open at the end of the previous reporting period (October 1, 2020–March 31, 2021).

¹⁰ This figure represents the sum of:

- (a) (U) The number of cases in which an active OIG investigation is still in process (i.e., 61), plus
- (b) (U) The number of cases for which OIG is awaiting final DIA management action in response to an earlier-published OIG Report of Investigation or Management Referral (i.e., 32).

¹¹ A summary of these cases can be found in the unclassified “Summaries of Published Investigative Reports” section of this report.

¹² See previous footnote.

¹³ See previous footnote.

¹⁴ A summary of these cases can be found in the unclassified and classified “Significant Management Referrals” sections in this report.

Table A-5: Investigative Activities

Description	Quantity
Hotline Program	
DIA OIG Hotline Contacts Received in Reporting Period ¹⁵	6,864
DIA OIG Hotline Contacts Closed in Report Period ¹⁶	6,633
DIA OIG Hotline Contacts Not Yet Viewed	6
DIA OIG Hotline Inquiries Opened in Reporting Period ¹⁷	225
DIA OIG Hotline Inquiries Closed in Reporting Period	149
Intelligence Oversight	
Cases Opened in Reporting Period	0
Cases Closed in Reporting Period	0
Cases Still Open at End of Reporting Period	0
Reports of Investigation Issued in Reporting Period	0
Referred to Management	0
Management Referrals	
Referrals in Reporting Period (external)	0
Referrals in Reporting Period (DIA management)	31
Referrals resulting from published Reports of Investigation	7
Referrals Resulting From Direct Referral Of Evaluated Complaints (I.E., DIA OIG Hotlines Inquiries/Not COVID-19 Related) To DIA Management	23
Referrals Resulting From Direct Referral Of Evaluated Complaint(S) (I.E., DIA OIG Hotline Inquiries/COVID-19 Related) To DIA Management	1

¹⁵ The term “contact” means an unevaluated complaint or request for information or assistance.

¹⁶ A “contact” is closed when the DIA OIG Hotline evaluates it and determines it did not merit further action.

¹⁷ When the DIA OIG Hotline evaluates a “contact” and determines it merits further action, an “inquiry” is opened so Hotline representatives can take additional action (e.g., directly address the matter itself, refer the matter to DIA management for information or action, or refer the matter to DIA OIG Investigations for further inquiry or investigation).

Table A-6: Summary of Recommendations as of September 30, 2021¹⁸

Description	Audits	Inspections and Evaluations	Investigations	Total
Open Recommendations	19	44	5	68
Closed Recommendations	11	0	4	15
Overdue Recommendations	14	29	1	44
Percentage Overdue of Open Recommendations	74%	66%	20%	

Table A-7: Overdue Recommendations Breakdown as of September 30, 2021

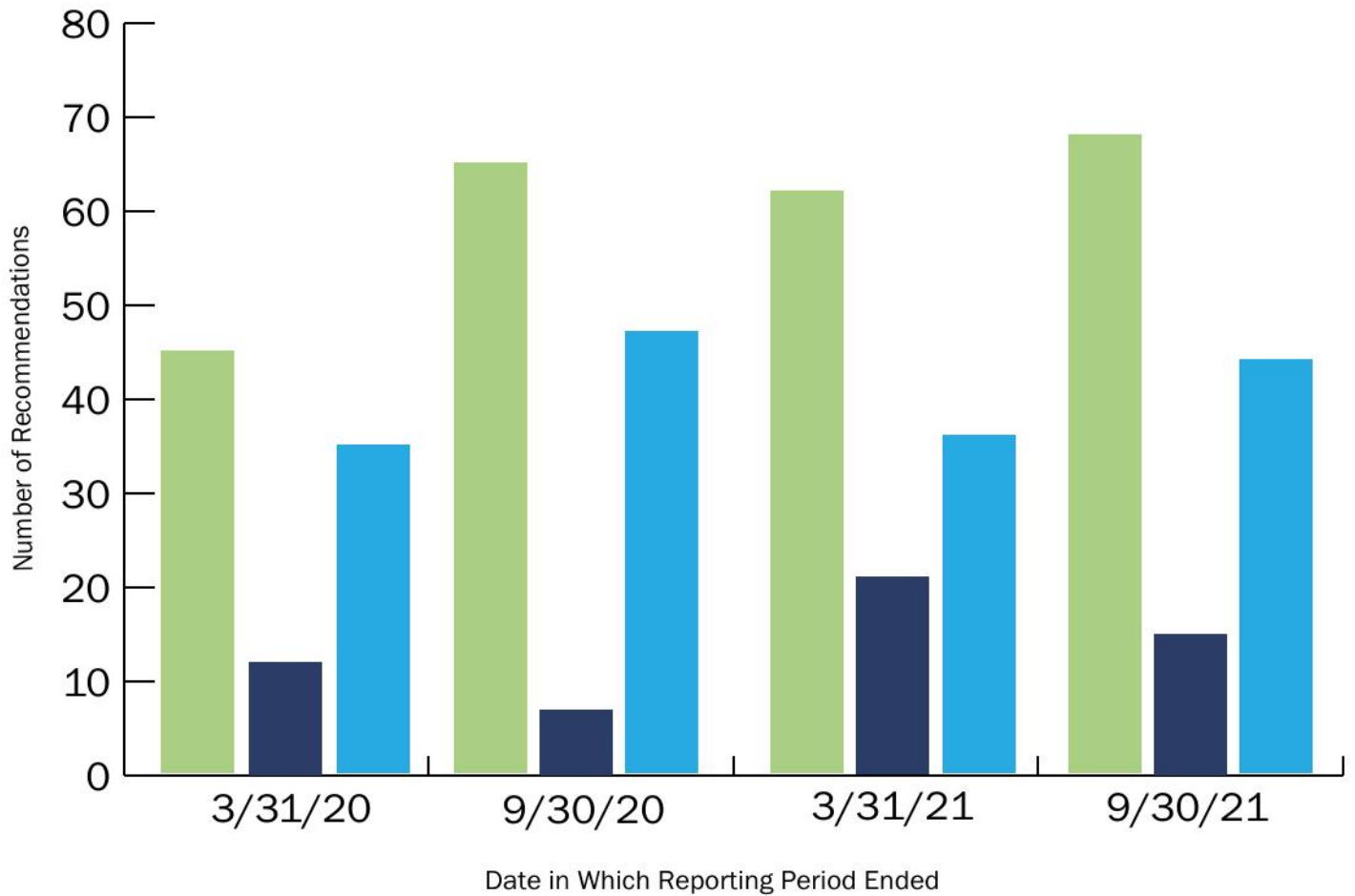
Description	Audits	Inspections and Evaluations	Investigations	Total
Less than 180 days	3	9	1	13
181-365 days	5	3	–	8
Greater than 365 days	6	17	–	23
Total	14	29	1	

¹⁸ “Overdue recommendations” refers to those recommendations that DIA management has not addressed within established timelines.

Table A-8: Recommendation Trends

Recommendation Trends

From March 31, 2020 to September 30, 2021



Legend:

- Open Recommendations
- Closed Recommendations
- Overdue Recommendations

Table A-9: Summary of Activities

Summary of Activities



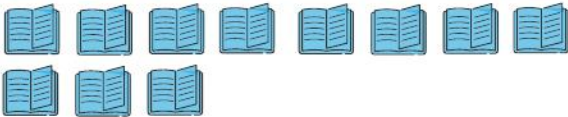
Expected Fraud Recoveries

\$44,893

Recommendations Issued this Period



Audits - 2



Inspections and Evaluations - 11



Investigations - 5

Recommendations Closed by Agency



Allegations



Substantiated Allegations

Appendix B. Status Recommendation Tables

Audits Division Recommendations

Table B-1: Audit of DIA’s Contract Requirements (2017-1005)

We audited whether DIA’s acquisition planning process resulted in complete and timely contract requirements. We determined that DIA’s acquisition planning efforts did not always start soon enough. Only 1 of the 14 contracts we reviewed met its planning milestone; the others missed the milestone by an average of 160 days, resulting in missed requirements, service gaps, and limiting time for contracting personnel to negotiate the best deal and comply with regulations. For example, in the process of replacing an expiring software contract, DIA missed a \$4.1 million discount because mission requirement owners began planning too late. Acquisition planning record (APR) preparation and review also needed improvement; 20 of the 29 APRs we reviewed had missing or non-compliant documentation, which increased the risk of untimely or incomplete requirements. Project results aligned with our DIA FY 2020 Top Management Challenge—Financial Management. We made four recommendations, three of which were closed in previous periods. Agency management is currently acting on the remaining open recommendation.

Rec. No.	Summary of Recommendation	Action Planned/Status
03	<p>The Office of the Chief Financial Officer (CFO), account for contract files by taking the following actions:</p> <p>a) Within 120 days of the final report, perform a risk assessment based on criteria including Federal Acquisition Regulation (FAR) section 4.805, “Storage, handling, and contract files,” to determine the appropriate scope for conducting an inventory of contract files.</p> <p>b) Within 1 year of the final report, perform the contract file inventory to determine what contract files are missing and take action to locate and account for them.</p>	<p>Management agreed with recommendations, completed part A of the recommendation, and is in the process of addressing part B.</p> <p>Status: Open</p>

Table B-2: Audit of DIA’s Unliquidated Obligations (2017-1006)

We audited whether DIA accurately recorded and processed obligation amounts, deobligated unliquidated obligations (ULOs) in a timely manner, and maintained valid and complete information to report ULO balances. We determined that DIA is unlikely to spend \$250 million of its FY 2017 appropriations, despite obligating nearly all funds that year. We also determined that fund holders did not deobligate an estimated \$377 million of the ULOs as of FY 2017 year-end, and we questioned \$4.8 million in payments due to improperly authorized vouchers. Project results aligned with our DIA FY 2020 Top Management Challenge—Financial Management. Management across DIA, including CFO and CIO, agreed with all 19 of our recommendations. The final two recommendations were closed this period, and all potential funds put to a better use were addressed.

Rec. No.	Summary of Recommendation	Action Planned/Status
03	The Directorate for Science and Technology (ST), within 120 days of the final report, develop and implement strategies for obligating funds to compensate for the effects of external factors and account for prior results in order to increase the use of appropriations. This may include, but is not limited to, shifting timelines to obligate funds earlier in the year, and considering external factors and prior results in cost estimates and spending plans.	Management has addressed the intent of the recommendation. Status: Closed
10	ST, within 180 days of the final report, develop and implement processes for fund holders to review purchase order lines and obligation status throughout the fiscal year outside of the triannual review process.	Management has addressed the intent of the recommendation. Status: Closed

Table B-3: Audit of DIA’s Incoming Reimbursable Orders (2018-1004)

We audited whether DIA’s incoming reimbursable orders were valid, aligned with Agency roles and missions, completed per agreement terms, and recorded accurately and in a timely manner. We determined that DIA processed valid incoming orders and senior leaders approved role and mission alignment. However, while Agency records agreed to the approved funding documents, we found some issues with cost estimates requirement definitions. Specifically, 42 orders, totaling approximately \$99 million, had no cost estimate or the estimate was inaccurate by an average of 99 percent of the order value. In addition, 25 orders, totaling almost \$31 million, did not specify DIA and customer requirements for fulfilling the agreement terms, including 13 orders where work began before receiving funding documents. Finally, 24 percent of the sampled orders took more than 60 days to process. Agency management was partially responsive to both our recommendations. Project results aligned with our DIA FY 2020 Top Management Challenge—Financial Management. We closed one recommendation during this reporting period, and Agency management is in the process of taking action on the other open recommendation.

Rec. No.	Summary of Recommendation	Action Planned/Status
01	CFO, within 180 days of the final report, revise and implement Agency policy and procedures for accepting orders, to include standards for developing, approving, and documenting cost estimates and customer requirements.	Management agreed with the recommendation and is in the process of implementing its corrective action plan. Status: Open
02	CIO, in coordination with the CFO, within 90 days of the final report, determine whether the practice of beginning DoD Intelligence Information System support services without an approved funding document is appropriate and take necessary corrective action based on that determination. Corrective action may include pursuing a policy exception for these situations (in coordination with DoD), holding personnel accountable for circumventing existing policy, or other actions.	Management has addressed the intent of the recommendation. Status: Closed

Table B-4: Audit of DIA’s Information Technology Services Contracts (2018-1006)

We audited whether information technology services acquired by DIA, as a service provider of IC Enterprise Management (EMT), were cost effective, properly funded, and administered in accordance with the IC IT Enterprise strategy. We determined that CFO awarded four task orders, totaling \$224 million that were not within the scope of the IC EMT contract, as required by regulation. Contracting officers made incorrect scope determinations, and none of CFO’s contract review processes were designed to detect or prevent out-of-scope work. Additionally, DIA did not properly administer the award fee, awarding payment of \$550,187, or 86 percent of the total award fee, even though the contractor did not meet requirements for the amount it received. Finally, DIA did not collect and analyze award and incentive fee data, as required by regulation. These internal control issues limited competition, reduced DIA’s leverage in negotiating contract prices, and did not meet the intended objective of the award fee, which is to enhance contractor performance. Project results aligned with our DIA FY 2020 Top Management Challenge—Financial Management. We made three recommendations, and two recommendations were closed in previous reporting periods. Management is in the process of taking action on the remaining open recommendation.

Rec. No.	Summary of Recommendation	Action Planned/Status
03	CFO, within 180 days of the final report, design and implement a process to collect and analyze relevant data on award and incentive fees paid to contractors. This should include, at a minimum, using the results of such analysis to evaluate the extent, use, and effectiveness of award and incentive fees in improving contractors’ performance and achieving desired program outcomes in accordance with FAR 16.401(f).	Management agreed with the recommendation and is in the process of implementing its corrective action plan. Status: Open

Table B-5: Audit of DIA’s Unplanned Price Changes, Project 2019-1006

We audited whether DIA performed appropriate and timely analysis to support unplanned price changes on DIA contracts between FYs 2018 and 2020, including changes in response to the COVID-19 pandemic. We determined that DIA policies, procedures, and reviews were not designed to assure proper proposal analyses for unplanned price increases, and DIA’s contracting system did not have the capability to identify and track said changes. DIA did not perform appropriate and timely analysis to confirm that 9 of 11 price increases (82 percent) we reviewed totaling \$11.2 million were fair and reasonable. Additionally, DIA could have saved \$176,000 for other mission priorities if it had analyzed and negotiated price escalation for option periods using data maintained by the Bureau of Labor Statistics. The project results aligned with our DIA FY 2020 Top Management Challenge—Financial Management. Management is in the process of taking action on the three recommendations.

Rec. No.	Summary of Recommendation	Action Planned/Status
01	CFO, within 180 days of the final report, update and implement policies and procedures to consolidate regulatory and other requirements for contract modifications that result in unplanned price changes. At a minimum, the policy and procedures should address appropriate and timely completion and documentation of required proposal analysis, preparation of Government estimates that are independent, and requirements and guidance for analyzing and negotiating escalation rates. Examples of implementation may include training, formal communication of updated policy and procedures, alerts, or other methods.	Management agreed with the recommendation and is in the process of implementing its corrective action plan. Status: Open
02	CFO, within 180 days of the final report, design and implement controls to monitor the appropriateness and timeliness of proposal analysis and associated supporting documentation for modifications that result in unplanned price changes. Actions could include additional procedures for independent contracting officer reviews for contract modifications, or other methods.	Management agreed with the recommendation and is in the process of implementing its corrective action plan. Status: Open
03	CFO, within 180 days of the final report, develop and implement a capability to identify and track unplanned modifications that result in unplanned price changes. This capability could assist CFO with monitoring unplanned price changes as part of their MICP, in accordance with Government Accountability Office (GAO) publication, GAO 14 704G, “Standards for Internal Control in the Federal Government,” September 2014.	Management agreed with the recommendation and is in the process of implementing its corrective action plan. Status: Open

Table B-6: Evaluation of DIA’s Implementation of CARES Act—Section 3610 (2020-1006)

We evaluated whether DIA’s contractor reimbursements under section 3610 of the Coronavirus Aid, Relief, and Economic Security (CARES) Act were appropriate and governed by language authorizing Federal agencies to reimburse contractors for leave given to keep their employees and subcontractors ready to ensure a timely return to work. We determined that DIA’s contractor reimbursement under section 3610 of the CARES Act did not meet all the requirements of the Act, as well as implementation guidance from the U.S. Office of Management and Budget (OMB) and DoD. For all 17 reimbursements we reviewed, DIA did not document how the pandemic affected a contractor’s status and did not modify the contracts to allow for reimbursements under section 3610 as required. DIA could not show that the 17 reimbursements we reviewed, totaling \$1.5 million, were appropriate, meaning all \$10.7 million CARES Act, section 3610 contractor reimbursements made through January 31, 2021, may not have been appropriate. Agency policies and procedures implementing section 3610 did not include the requirements for documenting contractors’ status as affected by the pandemic and modifying the contracts to authorize the reimbursements. We performed this evaluation in response to the COVID-19 pandemic. We made three recommendations, and closed two recommendations during the reporting period. Management is in the process of taking action on the remaining open recommendation.

Rec. No.	Summary of Recommendation	Action Planned/Status
01	CFO, within 90 days of the final report, determine whether all contractors reimbursed under section 3610 of the CARES Act were affected and document the contractors’ affected status in the contract. This action may include consideration of the Office of the Under Secretary of Defense “Memorandum for Record Template for CARES Act, Section 3610 Reimbursements” to document the affected status. For any contractor determined not to be affected, take appropriate corrective action with respect to any reimbursement already paid.	Management has addressed the intent of the recommendation. Status: Closed
02	CFO, within 90 days of the final report, for contractors determined to be affected in Recommendation 1, CFO modify the contract to allow for the reimbursement.	Management has addressed the intent of the recommendation. Status: Closed
03	CFO, within 90 days of the final report, update policies and procedures to require contracting officers to document contractors’ affected status in the contract file, and to modify the contract when implementing section 3610 of the CARES Act.	Management agreed with the recommendation and is in the process of implementing its corrective action plan. Status: Open

Table B-7: Evaluation of DIA’s Compliance with the Improper Payments Elimination and Recovery Act for Fiscal Year 2020 (2021-1005)

A summary of this report appears in the “Summary of Audits Division Activity” section of the Main Report. Project results aligned with our DIA FY 2020 Top Management Challenge—Financial Management. Management concurred with the recommendation and is taking action on the open recommendation.

Rec. No.	Summary of Recommendation	Action Planned/Status
01	CFO, within 90 days of the final report, conduct a program-specific risk assessment that meets OMB requirements for payment programs due for reassessment in FY 2020 and based on the results of the risk assessments, take appropriate action to address all other improper payment requirements listed in the previous bullets.	Management agreed with the recommendation and is in the process of implementing its corrective action plan. Status: Open

Inspections and Evaluations Division Recommendations

Table B-8: Evaluation of DIA’s Human Capital Services (2017-2008-HQ)

We evaluated the integrity of systems related to DIA’s human capital services, including processes, controls, and business rules, to assess their efficiency and effectiveness in managing human capital. We determined that OHR needs to develop and communicate a comprehensive human capital strategy to show customers and stakeholders how OHR enables the DIA mission and provides employee services. The project results aligned with our DIA FY 2020 Emerging Risk—Human Capital Strategy and Talent Management. We closed this evaluation on October 1, 2018; however, we reopened this evaluation in 2019 because the Agency had not developed and implemented a human capital strategy. We reissued and reassigned one recommendation, which remains open.

Rec. No.	Summary of Recommendation	Action Planned/Status
01	CS, establish, document, and implement a human capital strategy that aligns with DIA missions, readiness needs, and strategic objectives. Additionally, CS should establish an implementation and management plan that facilitates increased effectiveness, understanding, and accountability of human capital services delivery and processes.	Management agreed with this recommendation and is in the process of implementing its corrective action plan. Status: Open

Table B-9: Inspection of Personnel Accountability in Conjunction with Natural and Manmade Disasters (2018-2001-HQ)

We inspected the effectiveness of personnel accountability plans, procedures, reporting, and oversight of personnel accountability systems, including controls to monitor program compliance with DoD governance. We determined that DIA personnel accountability policies and practices effectively accounted for DIA civilian employees, assigned military members, and DoD-affiliated contractors in the event of a manmade or natural disaster. Additionally, we observed that the Agency successfully accounted for its personnel in affected locations during 44 real-world personnel accountability events and 2 exercises in 2017. The project results aligned with our DIA FY 2020 Emerging Risk—Human Capital Strategy and Talent Management. We issued three recommendations, two were closed in previous reporting periods and one remains open.

Rec. No.	Summary of Recommendation	Action Planned/Status
01	The Directorate for Mission Services (MS), develop and codify business systems and processes to provide continuous, accurate personnel accountability for all required DoD-affiliated personnel.	Management agreed with this recommendation and is in the process of implementing its corrective action plan. Status: Open

Table B-10: Evaluation of DIA’s Personnel Security Program (2018-2002- HQ)

We evaluated adjudication policies, processes, and practices for assessing, validating, and certifying applicant eligibility for access to national security information. We also evaluated Personnel Security Program interdependencies with other programs and offices that provided information for “whole person” consideration in adjudication decisions. Our evaluation did not address processes associated with periodic reinvestigations. We identified opportunities to enhance the Agency’s program and improve the effectiveness and efficiency of determinations on eligibility for access to sensitive compartmented information and other controlled access program information. The project results aligned with our DIA FY 2020 Top Management Challenge—Information Security Governance. We issued four recommendations, two were closed in previous reporting periods and two remain open.

Rec. No.	Summary of Recommendation	Action Planned/Status
01	MS, implement standardized initial and continuing training for adjudicators and case managers.	Management agreed with this recommendation and is in the process of implementing its corrective action plan. Status: Open
04	MS, develop an end-to-end Personnel Security Program process that integrates all stakeholder elements and clearly outlines roles and responsibilities, performance expectations, and milestones across all stakeholders.	Management agreed with this recommendation and is in the process of implementing its corrective action plan. Status: Open

Table B-11: Fiscal Year 2021 Report on Classification, (2021-2002)

A summary of this report appears in the “Summary of Inspection and Evaluation Activity” section of the Main Report. We issued seven recommendations, all of which remain open.

Rec. No.	Summary of Recommendation	Action Planned/Status
01	MS, in coordination with the Deputy Director for Global Integration and the Directorates for Analysis (DI), Operations, Intelligence (J2), and Science and Technology, review and update classification policy and internal controls to ensure uniform application of classification and handling markers across DIA finished intelligence reports. Certification Program against the program’s purpose and goals.	Management agreed with the recommendation and has provided an action plan. (U) Status: Open
02	DI, in coordination with J2, develop and implement processes and procedures to standardize pre-publication quality assurance reviews for classification and handling markers.	Management agreed with the recommendation and has provided an action plan. Status: Open
03	DI, in coordination with MS, update the DI security classification guides to meet current Executive, Federal, and IC requirements.	Management agreed with the recommendation and has provided an action plan. Status: Open
04	MS, develop and implement a scalable declassification strategy, with surge capacity, to achieve and maintain a baseline declassification review functionality and address DIA’s 28-year backlog of records overdue for automatic declassification review records, metrics, budgets, and contracts.	Management agreed with the recommendation and has provided an action plan. Status: Open

Table B-11: Fiscal Year 2021 Report on Classification, (2021-2002) Cont'd

Rec. No.	Summary of Recommendation	Action Planned/Status
05	MS, establish a Systematic Declassification Program in accordance with Executive, Federal, and DoD requirements.	<p>Management agreed with the recommendation and has provided an action plan.</p> <p>Status: Open</p>
06	MS, establish guidance for declassification priorities, review and update guidance for mandatory declassification review procedures, and establish internal controls to address risk to DIA's Mandatory Declassification Review Program.	<p>Management agreed with the recommendation and has provided an action plan.</p> <p>Status: Open</p>
07	MS, establish a process to periodically update the current list of authorized declassification personnel, and ensure that all declassification personnel are trained every 2 years, in accordance with applicable Federal law and IC, DoD, and DIA policy.	<p>Management agreed with the recommendation and has provided an action plan.</p> <p>Status: Open</p>

Table B-12: Management Alert on the Service Element Pay and Support for Personnel Assigned to the Defense Attaché Service, (2021-2005)

A summary of this product appears in the “Summary of Other Inspection and Evaluation Activity” section of the Main Report. Given the criticality of the identified issues, we requested Agency management provide us with corrective actions and/or a plan of action, to include activity milestones, they intend to take to address the issues. That action remains open.

Rec. No.	Summary of Recommendation	Action Planned/Status
01	Directorate for Operations (DO), in coordination with the Military Integration Office (MIO), provide us with corrective actions and/or a plan of action, to include activity milestones, they intend to take to address the issues. We also request notification when the Identified actions are complete.	Management’s response is pending. Status: Open

Investigations Division Recommendations

Table B-13: Reprisal and Abuse of Authority Investigation (2019-5043-01)

We investigated and substantiated allegations of reprisal and abuse of authority made by a DIA employee against three supervisory employees, one of whom was a DIA senior official. During our investigation, we identified two management deficiencies that, if addressed, could have precluded the involuntary reassignment of the DIA employee (a contributing factor in considering the complaint to represent reprisal and abuse of authority). Of note, although we identified two management deficiencies, we issued one recommendation, which remains open.

Rec. No.	Summary of Recommendation	Action Planned/Status
01	MS, ensure that the SEC personnel reassignments and Personnel Management Panel follow DIA instruction (DIAI) 1400.008, "Employment and Placement," April 24, 2015, and DIAI 1404.010, "Civilian Career Assignment Programs," November 23, 2015.	With management for consideration. Status: Open

Table is Unclassified

Table B-14: Travel Fraud and Misuse of Emergency and Extraordinary Expense Funds Investigation, Case 2019-005012-01

A summary of this report appears in the "Summary of Investigations Division Activity" section of the Main Report. We issued four recommendations to DIA management, which were subsequently closed during this period.

Rec. No.	Summary of Recommendation	Action Planned/Status
01	DO, ensure (DAS personnel operations are consistent and in compliance with DoD Manual (DoDM) 5220.22, volume (vol.) II ("National Industrial Security Program: Industrial Security Procedures For Government Activities"), September 30, 2020).	Management has addressed the intent of the recommendation. Status: Closed
02	DO, ensure DAS personnel operations are consistent and in compliance with DAS Instruction 100-1: e.g., DAS Instruction 100-1, vol. II, "Defense Attaché Service Administration, vol. II, Emergency and Extraordinary Expenses," December 31, 2014.	Management has addressed the intent of the recommendation. Status: Closed

Table B-14: Travel Fraud and Misuse of Emergency and Extraordinary Expense Funds Investigation, Case 2019-005012-OI Cont'd

Rec. No.	Summary of Recommendation	Action Planned/Status
03	DO, ensure DAS personnel are aware of overarching information assurance security principles as illustrated in relevant guidance (e.g., Chairman of the Joint CJCSI 6510.01F, "Information Assurance (IA) and Support to Computer Network Defense," February 9, 2011).	<p>Management has addressed the intent of the recommendation.</p> <p>Status: Closed</p>
04	DO, ensure DAS personnel follow the requirements for approval of Funded Environmental and Moral Leave travel as outlined in DX Publication 100-1 (e.g., DX Publication 100-1, vol. I, "Defense Attaché Service Administration, vol. I, Defense Attaché Office Administration," April 13, 2011).	<p>Management has addressed the intent of the recommendation.</p> <p>Status: Closed</p>

Appendix C. Audits, Inspections, Evaluations, and Investigations Closed Since April 1, 2021

Table C-1: Audits Closed Since April 1, 2021

Report No.	Date Closed	Summary
2017-1006	08/12/2021	Audit of DIA's Unliquidated Obligations. A summary of this report can be found in the "Status of Recommendations" section of the Main Report. We issued 19 recommendations, all of which are closed.

Table C-2: Investigations Closed Since April 1, 2021

Report No.	Date Closed	Summary
2017-005070-OI	04/15/2021	False Claims Investigation. On May 3, 2017, the U.S. Air Force (USAF) Office of Special Investigations (OSI) initiated an investigation into a U.S. contractor company allegedly having submitted false claims for cost reimbursements under its U.S. Government contracts. This subsequently became a joint case with the DoD OIG's Defense Criminal Investigative Service. Following initial investigative work, we did not develop sufficient evidence to support the complainant's initial claim to USAF OSI that the contractor company knowingly submitted false claims for costs reimbursements to the U.S. Government.

Table C-2: Investigations Closed Since April 1, 2021 Cont'd

Report No.	Date Closed	Summary
2019-005006-OI	06/24/2021	<p>Misuse of Government Resources and Violation of Privacy Act Investigation. In response to an earlier complaint, DIA OIG determined that a DIA employee (i.e., Subject) violated Agency guidance by having earlier removed documents containing PII of another DIA employee (their supervisor) from the DIA Headquarters building without an official reason. According to the Complainant, the Subject had removed the documents in order to respond to a proposed disciplinary action. Of note, during the course of our investigation, the Subject accused the other employee (their supervisor) of an abuse of authority. We subsequently determined that the supervisor had not retaliated or abused their authority against the Subject.</p>

Table C-2: Investigations Closed Since April 1, 2021 Cont'd

Report No.	Date Closed	Summary
2019-005007-OI	07/02/2021	<p>Misuse of Position Investigation. In response to an earlier complaint, DIA OIG determined three DIA employees violated title 5, C.F.R. § 2625.502, “Personal and Business Relationships,” and a fourth DIA employee violated title 5 C.F.R. § 2635.101(b)(11), “Basic obligation of public service.”</p> <p>The first employee violated title 5, C.F.R. § 2625.502 twice, once when they failed to advise their supervisors that their relatives were employed on contracts that supported the employee’s respective duty office, and a second time when they served as chairperson on a Source Selection Election Board, despite knowing their relative was previously employed by, and planned to seek future employment with, a company the board would evaluate.</p> <p>The second employee, (who earlier violated title 5, C.F.R. § 2625.502, when they failed to advise their supervisors that their relatives were employed on contracts that supported the employee’s respective duty office), also violated title 5, C.F.R. § 2635.702, “Use of public office for private gain,” on two separate occasions when they used their position to improperly influence contract companies.</p> <p>The third employee violated title 5, C.F.R. § 2625.502, when they failed to advise their supervisors that their relatives were employed on contracts that supported the employee’s respective duty office, and violated title 5, C.F.R. § 2635.101(b)(11), “Basic obligation of public service,” when they allowed the aforementioned employment activities to continue without reporting the improprieties to contracting officers or to general counsel.</p> <p>Lastly, the fourth employee violated title 5, C.F.R. § 2635.101(b)(11), “Basic obligation of public service,” when they allowed the aforementioned employment activities to continue without reporting the improprieties to contracting officers or to general counsel. The employees received the following:</p> <ul style="list-style-type: none"> • The first employee initially received an official Letter of Reprimand (LoR) on August 26, 2019. However, the LoR was subsequently withdrawn on December 9, 2019 in response to the employee having filed a formal grievance; • The second employee received an LoR on September 10, 2019; • The third employee received verbal counseling; and • The fourth employee retired from Federal service prior to the conclusion of our investigation. Consequently, DIA was unable to take disciplinary action.

Table C-2: Investigations Closed Since April 1, 2021 Cont'd

Report No.	Date Closed	Summary
2020-005026- OI	07/01/2021	<p>Theft of U.S. Government Property (Management Referral). We received a complaint alleging that a USAF civilian employee, working on a joint duty assignment with DIA, had routinely stolen IT equipment from Agency workspaces for his personal use. The complaint further alleged that between 2018 and 2019, the employee had officially acquired, but failed to properly account for approximately \$1.5 million in U.S. Government property. Based on our initial investigative efforts and subsequent corrective actions by DIA management, Agency management officials were able to locate, and properly account for all Agency property. Subsequently, DIA management officials implemented corrective actions to ensure proper accounting procedures would be in effect for future Agency acquisitions.</p>

Appendix D. Index of Reporting Requirements

Section	Semiannual Reporting Requirement	Page
4(a)(2)	Legislative and regulatory reviews	8
5(a)(1)	Significant problems, abuses, and deficiencies	10-23
5(a)(2-3)	Recommendations to correct significant problems, abuses, and deficiencies	32
5(a)(4)	Matters referred to prosecutive authorities and resulting prosecutions and convictions	16-23
5(a)(5)	Reports to the Director, DIA of refusals to provide information	6
5(a)(6)	List of reports issued during the reporting period	10-23
5(a)(7)	Summaries of significant reports	10-23
5(a)(8)	Statistical table showing questioned and unsupported costs	24
5(a)(9)	Statistical tables showing recommendations that funds be put to better use	25
5(a)(10) (A)	Summaries of reports previously issued that still lack management decision	24
5(a)(10) (B)	Summaries of reports previously issued that lacked management comment within 60 days	6
5(a)(10) (C)	Summaries of reports previously issued that have remaining unimplemented recommendations	32
5(a)(11)	Significant revised management decisions	6
5(a)(12)	Significant management decisions with which the IG disagrees	6
5(a)(13)	Federal Financial Management Improvement Act of 1996	6
5(a)(14-16)	Peer reviews	6
5(a)(17-18)	Investigations statistics and metrics	16
5(a)(19)	Investigations involving substantiated allegations against senior officials	16
5(a)(20) (A)	Descriptions of whistleblower retaliation	16
5(a)(20) (B)	Establishment imposed consequences of whistleblower retaliation	16
5(a)(20) (C)	Whistleblower retaliation settlement agreements	16
5(a)(21)	Attempts to interfere with IG independence	6
5(a)(22)	Public disclosure	6
6718(b)	National Defense Authorization Act of FY 2020	6

