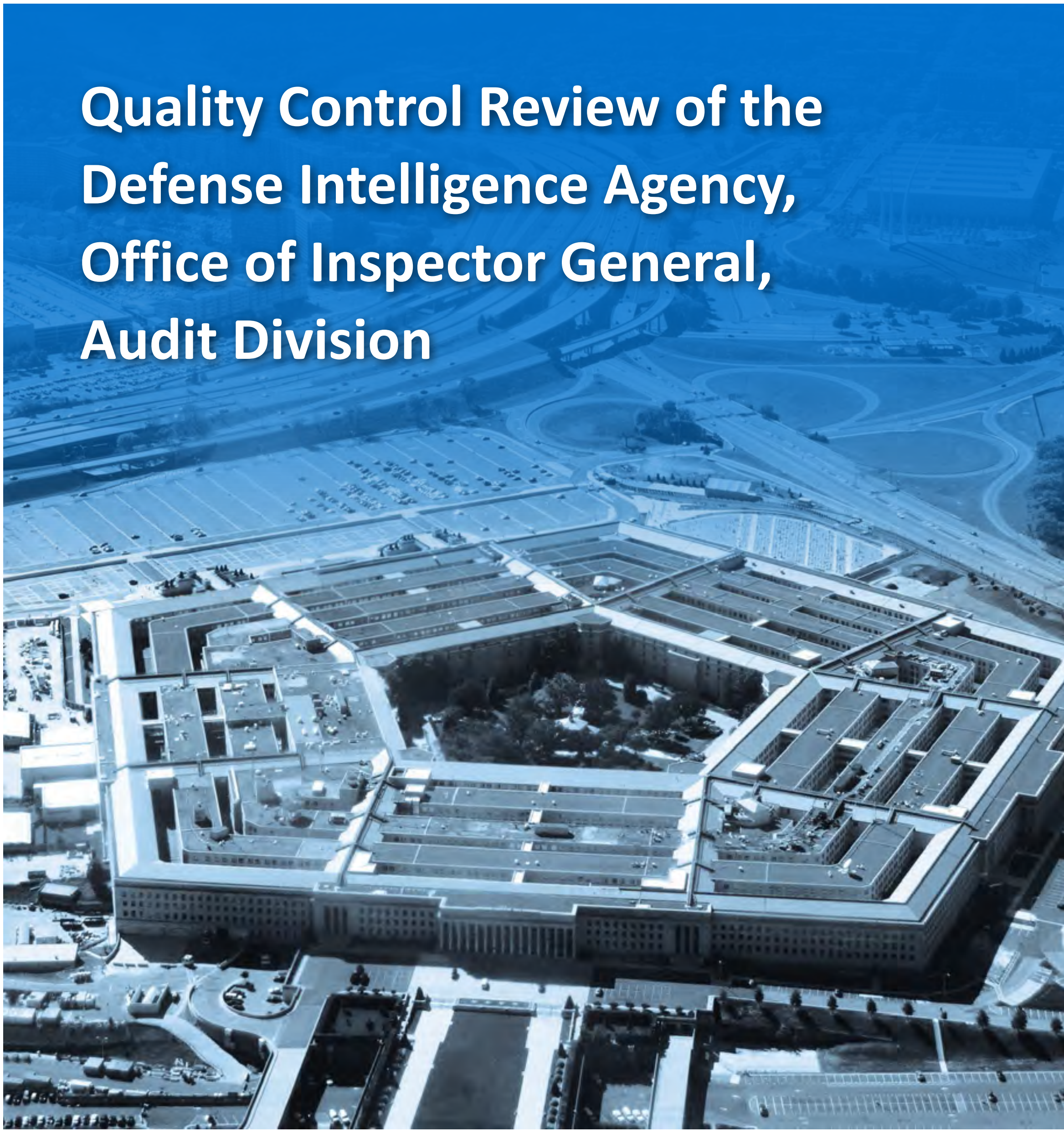
Report No. DODIG-2015-084

# Inspector General

*U.S. Department of Defense*

FEBRUARY 26, 2015



# Quality Control Review of the Defense Intelligence Agency, Office of Inspector General, Audit Division

INTEGRITY ★ EFFICIENCY ★ ACCOUNTABILITY ★ EXCELLENCE

INTEGRITY ★ EFFICIENCY ★ ACCOUNTABILITY ★ EXCELLENCE

## Mission

*Our mission is to provide independent, relevant, and timely oversight of the Department of Defense that supports the warfighter; promotes accountability, integrity, and efficiency; advises the Secretary of Defense and Congress; and informs the public.*

## Vision

*Our vision is to be a model oversight organization in the Federal Government by leading change, speaking truth, and promoting excellence—a diverse organization, working together as one professional team, recognized as leaders in our field.*

Fraud, Waste & Abuse
HOTLINE
Department of Defense
dodig.mil/hotline | 800.424.9098

For more information about whistleblower protection, please see the inside back cover.

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

February 26, 2015

MEMORANDUM FOR DIRECTOR, DEFENSE INTELLIGENCE AGENCY

SUBJECT: Quality Control Review of the Defense Intelligence Agency, Office of Inspector General, Audit Division (Report No. DODIG-2015-084)

We are providing this report for your information and use. We reviewed the Defense Intelligence Agency, Office of Inspector General (DIA OIG), Audit Division, system of quality control in effect for the period January 1, 2011 through April 30, 2014. A system of quality control for the DIA OIG audit organization encompasses the audit organization's leadership, emphasis on performing high quality work, and policies and procedures established to provide reasonable assurance of compliance with generally accepted government auditing standards (GAGAS). The DIA audit organization is responsible for designing a system of quality control and complying with its system to provide DIA management with reasonable assurance that its audits are performed and reported in accordance with GAGAS in all material respects. We conducted this review in accordance with the Council of Inspectors General on Integrity and Efficiency (CIGIE) Quality Standards for Inspection and Evaluation.

We tested the DIA OIG audit organization's system of quality control for audits to the extent considered appropriate. GAGAS require that an audit organization performing audits or attestation engagements or both have an appropriate internal quality control system in place and undergo an external quality control review at least once every 3 years by reviewers independent of the audit organization being reviewed. An audit organization's quality control policies and procedures should be appropriately comprehensive and suitably designed to provide reasonable assurance that they meet GAGAS requirements for quality control.

Federal audit organizations can receive a rating of *pass, pass with deficiencies,* or *fail*. In our opinion except for the deficiencies discussed in this report, the quality control system was suitably designed. However, the controls were not consistently followed during the peer review period ended April 30, 2014. Accordingly, we are issuing a "pass with deficiencies" rating on the DIA OIG Audit Division's quality control system for the review period ended April 30, 2014.

Appendix A contains deficiencies that provide the basis for the opinion rendered. Appendix B contains an overview from the interviews conducted. Appendix C contains the scope and methodology of the review.

We appreciate the courtesies extended to the staff. For additional information on this report, please contact Ms. Carolyn R. Davis at (703) 604-8877 (DSN 664-8877) or Carolyn.Davis@dodig.mil.

Randolph R. Stone
Deputy Inspector General
Policy and Oversight

# Contents

## Introduction

## Appendixes

## Management Comments

# Introduction

## Defense Intelligence Agency

The Defense Intelligence Agency (DIA) became operational on October 1, 1961, as the Nation's primary producer of foreign military intelligence. DIA's mission is to satisfy the military and military-related intelligence requirements of the Secretary and Deputy Secretary of Defense, the Chairman of the Joint Chiefs of Staff, and the Director of National Intelligence. DIA provides the military intelligence contribution to national foreign intelligence and counterintelligence. DIA plans, manages, and executes intelligence operations during peacetime and crisis. DIA serves as the DoD lead for coordinating intelligence support to meet combatant commands' requirements; lead efforts to align analysis, collection, and intelligence, surveillance, and reconnaissance activities with all intelligence operations; and link and synchronize Military, Defense, and National Intelligence capabilities.

## DIA Office of Inspector General, Audit Division

The DIA Office of Inspector General's (OIG) mission is to support the overall DIA OIG role of providing oversight of and reporting upon matters, which pertain to the performance of mission and state of discipline, economy, and efficiency of the DIA. The audit staff's primary function is contract performance, financial statement and financial-related audits of DIA activities and programs world-wide. The DIA Inspector General reports to the Director of DIA. The Assistant Inspector General for Audit (AIGA) reports to the DIA Inspector General. In 2011, the DIA OIG Audit Division reorganized and implemented three distinct branches: Acquisition and Contracting, Financial Management, and Financial Statement Audits. On December 29, 2012, the Audit Division established the position of Quality Assurance Manager.

# Appendix A

## Deficiencies that Provide the Basis for the Opinion Rendered

Except for the deficiencies described below, the DIA OIG Audit Division's system of quality control in effect for the period ended April 30, 2014, was suitably designed to provide DIA OIG Audit Division with reasonable assurance of performing and reporting in conformity with applicable professional standards in all material respects.[1] However, the staff of the DIA OIG Audit Division did not always comply with the system of quality controls to provide reasonable assurance of compliance with generally accepted government auditing standards (GAGAS). Therefore, the DIA OIG Audit Division has received a peer review rating of pass with deficiencies.

We judgmentally tested the reports for compliance with GAGAS and the DIA OIG Audit Division's policies in nine areas: quality control and assurance, independence, professional judgment, competence, planning, evidence, documentation, supervision, and reporting.

## Quality Assurance Program

The Audit Division established its Quality Assurance Program in May 2012 and implemented it on January 1, 2013. The DIA OIG Audit Divisions, Quality Assurance (QA) Manager completed the first annual analysis and summary of monitoring procedures for the period ended December 31, 2013. The QA Manager reported the results of the review in the May 28, 2014, "DIA OIG Quality Assurance Annual Summary," report. The QA Manager reported on two technical reviews[2] and one quality control review. For Project 2013-100001-OA, "DIA Compliance with the Improper Payments Elimination and Recovery Act of 2010," March 15, 2013 (the FY 2012 IPERA audit), the QA Manager performed both a technical review and a quality control review. The QA Manager reported on the results of this review on September 16, 2013, "Final Report on Internal Quality Assurance Review of DIA Compliance with the Improper Payments Elimination and Recovery Act

[1] The deficiencies identified did not rise to the level of a significant deficiency because they were not systemic, and taken as a whole, were not significant enough to affect the DIA OIG Audit Division's reasonable assurance of performing and/or reporting in conformity with applicable professional standards in all material respects.

[2] The DIA OIG Audit Division's Audit Handbook Chapter 1, "General Standards," Section 1.4, "Quality Control and Assurance, Quality Assurance Program, Technical Reviews," provides that the primary purpose of technical reviews is to determine whether audit reports comply with GAGAS reporting standards and DIA OIG policies and procedures. Specifically, the reviewer determines whether the report addresses all objectives, describes scope and methodology thoroughly, presents results consistently throughout (for example, numbers do not change format or amount, mathematical calculations are correct), draws conclusions that follow from the details provided, and matches recommendations to the results. The Reviewer does not review supporting documentation to determine the level of compliance with GAGAS or if facts in the report are supported. Refer to the DIA IG Audit Division Quality Assurance Program Standard Operating Procedures on the Audit SharePoint Site (under Internal Guidance) for details on the technical review.

of 2010, Project No. 2013-100001-QA." This is one of the three audits that we selected for this peer review. From our review of the two quality control reports, we determined that the QA reviewer reported the same or similar matters that we identified during this peer review. The QA reviewer identified matters in the following areas:

- Independence – GAGAS Conceptual Framework Approach to Independence;
- Fieldwork Standards – Planning (Audit Risk, Identifying Sources of Evidence, Understanding the Nature of the Program, and Assessing Fraud Risk);
- Fieldwork Standards – Supervision;
- Fieldwork Standards – Evidence;
- Reporting Standard; and
- Quality Control Policies and Procedures.

As emphasized throughout this report, we found DIA OIG's Audit Division's Quality Assurance Program generally effective from its inception through April 30, 2014. In a memorandum dated September 4, 2013, "Response to Draft Report on Internal Quality Assurance Review of DIA Compliance with the Improper Payments Elimination and Recovery Act of 2010, Project No. 2013-100001-QA," the AIGA agreed with the QA reviewer's deficiencies. In the two IPERA audits, although the reliability of the reported findings was not affected, we are concerned about the sufficiency of the Audit Division's methodology for auditing DIA's compliance with IPERA for future IPERA audits. Both the DIA OIG Audit Division's QA review and this peer review identified similar deficiencies with the audit methodology as discussed throughout this report. In the two IPERA audits, the DIA OIG Audit Division auditors found that DIA did not comply with the IPERA. For the FY 2012 IPERA audit, the Audit Division reported the finding that DIA did not report on IPERA Program in the FY 2012 Agency Financial Report. For 2014-100000-OA, "DIA's Compliance with the Improper Payments Elimination and Recovery Act of 2010," April 14, 2014 (the FY 2013 IPERA audit), the Audit Division reported that DIA did not use a statistically valid methodology as IPERA requires.

## Independence

### *Conceptual Framework Approach to Independence Not Followed*

For two of the three audits reviewed, the auditors did not follow the GAGAS conceptual framework for independence. GAGAS 3.07 establishes a conceptual framework that auditors use to identify, evaluate, and apply safeguards to address threats to independence. On October 1, 2012, DIA OIG Audit Division issued Interim Guidance: Implementing the New GAGAS Independence Standards, including the requirement for GAGAS Conceptual Framework Approach to Independence. Although no impairments to independence were identified, the DIA OIG Audit Division did not follow the DIA OIG Audit Division's policy and apply the GAGAS conceptual framework for two of three audits reviewed. For Project 2012-100001-OA, "DIA's Capital Equipment Replacement Program (CERP)," June 17, 2013, (the CERP audit), the auditors applied the conceptual framework on the report issuance date. In addition, for the FY 2012 IPERA audit, the auditors did not document their conclusion from their brainstorming session. Additionally, the auditors did not apply the conceptual framework at the organization and audit levels.[3]

Moreover, the DIA OIG Audit Divisions' Audit Handbook does not provide guidance for disclosing threats to independence identified after issuance of the report. GAGAS 3.26 states that if a threat to independence is initially identified after the auditors' report is issued, the auditor should evaluate the threat's impact on the audit and on compliance with GAGAS.

By not complying with GAGAS' conceptual framework approach, reasonable and informed third parties might conclude that the auditors are not independent and did not exercise objective and impartial judgment on all issues in conducting the audit and reporting on the work.

In a memorandum dated May 28, 2014, the QA Manager reported a similar concern regarding the DIA OIG Audit Division's application of GAGAS' conceptual framework. Additionally, in a memorandum dated September 16, 2013, the QA Manager reported that for the FY 2012 IPERA audit, the team did not meet all of the requirements for conducting a project-level brainstorming session to identify, evaluate, and address threats posed to auditor independence as required by the Audit Division's interim guidance. The AIGA responded that the Audit Handbook would be revised to clarify procedures for assessing independence at the project and individual level during audit planning and to include processes for reassessing independence (at both the project and individual levels) during the fieldwork phase of the audit.

While DIA OIG, Audit Division's staff should improve application of the conceptual framework approach to independence at the audit level, DIA OIG officials stated that application of the conceptual framework approach has improved based on compliance in the third audit reviewed.

[3] GAGAS 3.08 states that auditors should apply the conceptual framework at the audit organization, audit, and individual auditor levels. GAGAS 3.10, states, in part, that for the purposes of independence evaluation using the conceptual framework, an audit organization that includes multiple offices or units, or includes multiple entities related or affiliated through common control, is considered to be one audit organization.

## Planning

### *Information Systems Controls Not Evaluated*

For two of three audits reviewed, the auditors did not evaluate the effectiveness of significant information systems controls that were needed to obtain sufficient, appropriate evidence to support the audit conclusions. GAGAS 6.25 states that audit procedures to evaluate the effectiveness of significant information systems controls include (1) gaining an understanding of the system as it relates to the information and (2) identifying and evaluating the general, application, and user controls that are critical to providing assurance over the reliability of the information required for the audit. Additionally, GAGAS 6.27 states that auditors should determine which audit procedures related to information systems controls are needed to obtain sufficient, appropriate evidence to support the audit findings and conclusions and provides factors for the auditors to consider in making this determination. The Audit Division's Audit Handbook, Chapter 3 "Project Execution, Other Planning Factors, Information System Controls" provides, in part, that if the information systems controls are determined significant to the audit objectives, auditors should evaluate the design and operational effectiveness of such controls.

DIA reported significant deficiencies in its information systems and reported that the system generated unreliable data in its FY 2012 and FY 2013 Statement of Assurance.[4] One of the deficiencies that DIA reported pertained to the inability of its Financial Accounting and Corporate Tracking System (FACTS), to account for financial data, such as account payable transactions, on the accrual basis of accounting.

Although the auditors used payment data in the two IPERA audits, they did not perform any procedures to evaluate the effectiveness of controls for accounts payable for DIA's IPERA Program. Additionally, the DIA officials represented that DIA uses two systems, the Contract Management System (CMS) and the FACTS, for accounts payable transactions. The auditors used financial data from the FACTS for the two IPERA audits. Specifically, for the FY 2012 IPERA audit and for the FY 2013 IPERA audit, the auditors did not gain an understanding of the system including the system used for accounts payable. Consequently, the auditors did not determine which audit procedures, related to information systems controls, were needed to obtain sufficient, appropriate evidence for determining whether DIA complied with IPERA.

[4] Revisions to OMB Circular A-123, VI.B Section 2, "Management's Responsibility for Internal Control, Reporting on Internal Control, Reporting Pursuant to Section 2." 31 U.S.C. 3512(d) (2), requires that annually the head of each executive agency submit to the President and the Congress (i) a statement on whether there is reasonable assurance that the agency's controls are achieving their intended objectives; and (ii) a report on material weaknesses in the agency's controls.

## *Computer-Processed Data Not Assessed*

For two of three audits reviewed, the auditors did not assess the validity and reliability of computer processed-data. GAGAS 6.57 states that in assessing the overall appropriateness of evidence, auditors should assess whether the evidence is relevant, valid, and reliable. Similarly, GAGAS 6.66 states that auditors should assess the sufficiency and appropriateness of computer-processed information regardless of whether this information is provided to auditors or auditors independently extract it. The DIA OIG Audit Division's Audit Handbook, Chapter 3, "Project Execution, Validating and Reliability of Data from a Computer Based System," provides for auditors to assess the reliability of computer-processed data if findings or recommendations are based on the data. Additionally, the Government Accountability Office (GAO) GAO-09-680G, "Assessing the Reliability of Computer-Processed Data, Preface" states that appropriateness includes validity and reliability, which in turn includes the completeness and accuracy of the data.

DIA reported that specific financial data, including general ledger and account payable amounts, are unreliable in the FY 2012 and FY 2013 Statements of Assurance. Although the auditors relied on financial reports from FACTS they did not assess the validity and reliability of the computer processed data in the two IPERA audits. For both IPERA audits, the auditors compared DIA reported financial data to amounts in the DIA-provided spreadsheets that contained accounts payable transactions. Specifically, for the FY 2012 IPERA audit the auditors used the FY 2011 accounts payable reports and data published in the DIA's September 30, 2012, "DIA IPERA Summary of Results-Baseline," report. For the FY 2013 IPERA audit, the auditors compared the data to amounts that DIA published in its Agency's Financial Report for FY 2013.

Additionally, the Audit Division's guidance states that auditors are required to test for reliability items like databases if the finding or recommendation is based on the computer processed data. The guidance in the Audit Division's Audit Handbook, Chapter 3, "Project Execution, Validating and Reliability of Data from a Computer Based System" does not emphasize that the reliability and validity of computer-processed data should be assessed early in the audit. The auditors are required to assess the reliability of computer-processed data early in the audit in order to use the results to design the appropriate steps and audit procedures and to gather the appropriate evidence. The GAO-09-680G, Section 5, "Assessing the Reliability of Computer-Processed Data, Planning a Data Reliability Assessment, Timing an Assessment" states, in part:

> Generally, a data reliability assessment is performed as early as possible on a project, preferably during the design phase. The audit plan helps by reflecting data reliability issues and any additional steps that still need to be taken in assessing the reliability of critical data. The audit team generally takes initial steps to test the data and review existing information about the data and the system that produces them before making the audit plan final.

The AIGA stated that the DIA OIG Audit Division is currently revising its audit policies and procedures with regard to assessing computer-processed data to strengthen the work performed in the area.

## *Understanding of Internal Controls Relative to the Audit Objective Not Sufficiently Assessed*

For the two IPERA audits, the auditors did not sufficiently assess audit risk by gaining an understanding of the internal controls within the context of the audit objective.  GAGAS 6.11b states that auditors should assess audit risk and significance within the context of the audit objectives by gaining an understanding of the internal controls as it relates to the specific objectives and scope of the audit.  The DIA OIG Audit Division's Audit Handbook Chapter 3 "Project Execution, Other Planning Factors, Internal Controls" provides that the team must obtain an understanding of internal controls that are relevant to the objectives of the audit. The policy further provides that at a minimum, to gain an understanding of the internal controls of the program, the audit team should:

- assess the organization's self-evaluation process to determine whether the area being audited is covered by the internal controls;
- identify internal controls related to the stated audit objectives, and assess whether the internal controls have been properly designed and implemented; and
- conduct limited testing of key internal controls.  Generally, the internal controls to be tested will be those needed to achieve the management's objective(s).

For both of the IPERA audits, in planning, the auditors decided to limit their understanding of the internal controls for DIA's IPERA Program to DIA's accounts payable process. DIA reported, in its FY 2012 and FY 2013 Agency Financial Report, increased risk due to its outsourcing accounts payable activities. Similarly in the FY 2012 and FY 2013 Statement of Assurance DIA reported that due to inadequate business processes and system limitations, amounts reported on DIA financial statements for Accounts Payable remain unreliable. For the FY 2012 IPERA audit, the auditors documented that the internal control weaknesses within the procure-to-pay or accounts payable process will not affect DIA OIG Audit Division's finding(s), results, or recommendation(s). The auditors did not design audit procedures to determine the effect of the reported internal control deficiencies on the audit objective for the two IPERA audits. In addition, for the FY 2013 IPERA audit, the auditors documented that they obtained an understanding of the internal controls related to the DIA accounts payable process for the three programs identified as susceptible to significant improper payments. However, the auditors did not design procedures to reduce the risk specific to the objectives and scope of the audit. In this audit, the auditors selected 40 transactions for testing. However, the working paper did not contain audit documentation that the auditors designed the sampling methodology to reduce audit risk. Instead, the auditors selected the number of transactions based on a decision to perform some testing in order to issue the report on time.

During this peer review, the AIGA responded that the DIA OIG, Audit Division is currently revising its audit policies and procedures with regard to assessing internal controls and audit risk to strengthen the work performed in the area. The AIGA also stated that DIA OIG, Audit Division has taken steps to improve auditors' understanding and documentation of sampling for audit testing. Specifically, the AIGA stated that selected auditors attended statistical sampling training in order to improve the auditors understanding and documentation of sampling for audit testing.

## *Terms of Service Provider Agreements Not Understood*

The DIA OIG Audit Division's auditors did not gain an understanding of contract terms while assessing audit risk. GAGAS 6.11d states, in part, that auditors should assess audit risk and significance within the context of the audit objectives by gaining an understanding of the provisions of contracts that are significant within the context of the audit objectives. The DIA OIG Audit Division's Audit Handbook Chapter 3, "Project Execution, Other Planning Factors, Potential Illegal

Acts or Fraud" states that the team's assessment of risk includes consideration of whether the entity has controls that are effective in preventing or detecting violation of laws, regulations, grant agreements, and provisions of contracts. For the FY 2012 IPERA audit and the FY 2013 IPERA audit, the auditors did not review the DIA service provider agreements so they could obtain an understanding of the agreement terms in their assessment of audit risk. DIA entered into service provider agreements with three different Government agencies to make payments on behalf of DIA. In another instance, the auditors did not determine whether a contractor submitted the invoice in accordance with the invoicing instructions in the contract. Specifically, for the FY 2013 IPERA audit, to provide feedback to the Chief Financial Officer on the accuracy of its review of payments reported as improper, the auditors selected and tested 40 transactions. For one transaction the contractor submitted the invoice on the Standard Form (SF) 1034, "Public Voucher for Purchases and Services Other than Personal.[5]" Although the contractor submitted the "Public Voucher for Purchases and Services Other than Personal," the auditors agreed with DIA that the contractor did not submit an invoice and then identified the payment as improper. The auditors did not document the form of invoice that the contract required the contractor to submit. The auditors are required to obtain an understanding of the contract terms in order to design steps to detect non-conformances, if any, with contract terms and requirements. By reviewing the contract invoicing terms, the auditors would be able to confirm whether the contractor complied with contract terms by requesting payment on the SF 1034.

## *Nature and Profile of the Program Not Understood*

In two of three audits reviewed, the auditors did not obtain an understanding of the nature and profile of the program. GAGAS 6.13 states that auditors should obtain an understanding of the nature of the program or program component under audit. GAGAS 6.15 states that obtaining an understanding of the program under audit helps auditors to assess the relevant risks associated with the program and the impact of the risks on the audit objectives, scope, and methodology. The Audit Division's Audit Handbook, Chapter 3, "Project Execution, Other Planning Factors, Nature of the Program and User Needs" provides, in part, in planning projects the team should consider the significance or the relative importance of actions or operations to the objectives and to potential users of the report. Auditors are required to obtain an understanding of the nature and profile of the program to help them assess the relevant risks associated with the program and the impact of the risks on the audit objectives, scope, and methodology.

[5] SF 1034 is an invoice or a public voucher that can be used for purchases and services that are not personal. The Federal Acquisition Regulations (FAR), updated through November 13, 2014, provides a copy of the form at FAR 53.301-1034.

For the FY 2012 IPERA audit and for the FY 2013 IPERA audit, the auditors documented their understanding of the accounts payable process instead of DIA's IPERA Program. By understanding the nature of the program the auditors would be able to assess risk to the program, design audit procedures based on the outcome of the assessment, and identify appropriate evidence based on the program risks.

On September 16, 2013, for the quality assurance review of the FY 2012 IPERA audit, the QA Manager identified the same issue. Specifically, the QA Manager reported that one planning working paper focused on the accounts payable process. The QA Manager also reported that since the objective of the audit was to assess DIA's compliance with IPERA, the basis of the planning working paper would typically be to understand the program the agency had in place to ensure compliance. However, the QA Manager reported, after discussions with the auditors, that the auditors decided that DIA did not have an IPERA Program and attributed the deficiency to insufficient documentation. Moreover, in reaching this conclusion, the DIA OIG Audit Division staff did not consider that DIA had already reported on its baseline assessment of the IPERA Program in the DIA report dated September 30, 2012.

Due to the QA reporting on an audit documentation deficiency, the AIGA responded on the same. The AIGA responded in the memorandum dated September 4, 2013, "Documentation of Management Discussions," that discussions had taken place with the audit managers. The AIGA also responded that discussions would continue in order to remind the audit managers that they need to document all meetings in which decisions related to the audit are made. Additionally, a standard working paper would be created that will require the audit managers to maintain a record of conversations with management when there is an impact to the audit.

## Audit Evidence and Documentation

### *Assurance Over the Reliability of DIA Provided Information Not Obtained*

For two of three audits reviewed, auditors did not obtain assurance over the reliability of the information provided by DIA officials. GAGAS 6.65 states that when auditors use information provided by officials of the audited entity as part of their evidence, they should determine what the officials of the audited entity or other auditors did to obtain assurance over the reliability of the information. The Audit Division's Audit Handbook, Chapter 3, "Fieldwork Phase, Project Execution, Audit Evidence, Data Gathering" states that the audit team should determine what the officials of the audited entity did to obtain assurance over the reliability of the information.  The auditors did not document what the Chief Financial Officer's staff did to obtain assurance over the reliability of the accounts payable data on which DIA reported.  In the two IPERA audits the auditors compared data that the officials provided in spreadsheets to amounts reported.  In the FY 2012 IPERA audit the auditors obtained spreadsheets containing FY 2011 amounts and compared the figures to amounts that DIA reported in its IPERA Program baseline assessment report dated September 30, 2012.  Similarly for the FY 2013 IPERA audit, the auditors compared figures to amounts that DIA reported in its FY 2013 Agency Financial Report.  Had the auditors understood what the officials did to obtain reliability for the financial data, the error that they found in their recalculation procedure might have been discovered earlier.

## *Procedures to Detect Fraud Not Designed*

For the FY 2012 IPERA audit and for the FY 2013 IPERA audit, the auditors did not design and perform procedures to detect fraud.  GAGAS 6.31 states that when auditors identify factors or risks related to fraud that has occurred or is likely to have occurred that they believe are significant within the context of the audit objectives, they should design procedures to obtain reasonable assurance of detecting any such fraud.  The Audit Division's Audit Handbook, Chapter 3, "Project Execution, Illegal Potential Acts or Fraud," requires auditors to design procedures to provide reasonable assurance of detecting such fraud.  The auditors did not follow the Audit Division's policy even though DIA had reported in its FY 2012 and FY 2013 Agency Financial Report that reliance on other agencies to process payments on its behalf increases the risk of fraud.  In both audits instead of designing procedures to increase fraud detection, the auditors concluded that they would be vigilant and assess the risk of fraud throughout the audit.  The auditors did not design procedures to determine whether fraud may have occurred as discussed in GAGAS 6.32.  Specifically, GAGAS 6.32 states when information comes to the auditors' attention indicating that fraud, significant within the context of the audit objectives, may have occurred, auditors should extend the audit steps and procedures, as necessary, to determine whether fraud has likely occurred and if so determine its effect on the audit findings.  If the fraud that may have occurred is not significant within the context of the audit objectives, the auditors may conduct additional audit work as a separate engagement, or refer the matter to other parties with oversight responsibility or jurisdiction.

In planning, the auditors documented that DIA's core accounting system lacks sufficient automated system controls, functionality, and validation processes of transactions processed from the systems used to process DIA disbursements; DIA's inability to obtain adequate documentation related to disbursements processed by DFAS (Defense Finance and Accounting Services); and DIA's limited involvement in its disbursement process makes DIA's disbursements susceptible to fraud, waste, and mismanagement. The auditors concluded that they would be vigilant and assess the risk of fraud throughout the audit. However, we did not identify where the auditors were vigilant and assessed fraud risk throughout the audit. Had the auditors sufficiently assessed the risk of fraud, they could have designed the appropriate steps in order to provide reasonable assurance of detecting fraud, had it occurred.

On September 16, 2013, the QA Manager reported that while assessing fraud risk continues throughout the audit, these risks should have been addressed during planning, to ensure that adequate procedure were designed to provide reasonable assurance that fraud would be detected, if it had occurred. The AIGA responded that work paper templates would be developed to assist auditors in documenting the audit and fraud risk assessment in planning and throughout the audit. The AIGA also responded that the Audit Handbook would be revised.

## *Testimonial Evidence Not Evaluated and Corroborated*

For two of three audits, the auditors did not evaluate the objectivity, credibility, and reliability of the testimonial evidence and corroborate testimonial evidence with documentary evidence. GAGAS 6.62 states that auditors should evaluate the objectivity, credibility, and reliability of the testimonial evidence. GAGAS 6.62 also states that documentary evidence may be used to help verify, support, or challenge testimonial evidence. Guidance on testimonial evidence appears in Chapter 3, "Project Execution" and Chapter 4, "Reporting" of DIA OIG's Audit Handbook. However, we did not find in the Audit Handbook guidance for the auditors to evaluate the objectivity, credibility, and reliability of testimonial evidence. Had the auditors used the testimonial evidence in interpreting or corroborating the documentary evidence, the evidence would have been of higher quality.

For the FY 2012 IPERA audit, the auditors did not corroborate the DIA officials' representation. In one instance, the auditors did not corroborate the official representation regarding the start of the accounts payable process. The officials represented that the process starts at the directorate level. In another instance, the auditors did not corroborate the DIA's methodology for downloading financial data from FACTS using the "Query Manager." Instead, the auditors relied on representations that DIA officials reported in the baseline IPERA Program risk assessment report dated September 30, 2012, and answers that DIA provided in response to their inquiries. In addition, for the FY 2013 IPERA audit, the auditors did not corroborate DIA statements. In one representation the official stated that the National Security Agency did not include payments made on DIA's behalf in its IPERA Program and that the Defense Financial and Accounting Services included the payments made on DIA's behalf in its IPERA Program. The auditors also did not confirm FY 2013 payments made on behalf of DIA by three different agencies. Instead, the auditors relied on representations reported in DIA's Agency Financial Report and information that they obtained from their inquiries.

The QA Manager reported on September 16, 2013, that a number of report references were made to testimonial evidence documented in meeting working papers; however, meeting working papers were not referenced to supporting documentation, or corroborated by review of documentary evidence where needed. The QA Manager also reported, that relying solely on testimonial evidence that is not corroborated or supported places the auditors' objectivity and credibility at risk. Additionally, in the memorandum dated May 28, 2014, the QA Manager reported that the audit team should carefully evaluate testimonial evidence to ensure its reliability and credibility in supporting findings and conclusions. The AIGA responded that the topic would be included when standard working papers are developed. The AIGA agreed that the audit teams need to improve planning related to the identification of types of evidence and assess the likelihood that sufficient, appropriate evidence will be available.

## Reporting

### *Scope and Methodology Not Fully Reported*

For two of the three audits reviewed, we identified concerns with the scope and methodology reported for addressing the audit objective. GAGAS 7.09 states that auditors should include in the report a description of the audit objectives and the scope and methodology used for addressing the audit objectives. Report users need this information to understand the purpose of the audit, the nature and extent of the audit work performed, the context and perspective regarding what is reported, and any significant limitations in audit objectives, scope, or methodology. The Audit Division's Audit Handbook Chapter 4, "Reporting, Objectives, Scope and Methodology," provides that the report must address the objectives, scope, and the methodology or approach used in conducting the audit. It also provides that the team must precisely describe the entity that was evaluated (organization, program, activity, or function) so that the report does not imply greater coverage than was actually provided. Chapter 4, "Reporting, Scope, Limitations," provides that the team should explicitly state any limitations of the scope (such as items not examined that one might infer or items specifically excluded), the reasons for the limitations, and the possible effects on audit results.

For the FY 2012 IPERA audit, the auditors did not identify any specific procedures that the IPERA law and implementing guidance required the Inspectors General to perform when determining whether the agency complied with IPERA reporting requirements. The auditors did not report, in the Scope and Methodology section, their scope limitation for not validating the accuracy and completeness of the FY 2011 computer-processed data. DIA OIG, Audit Division included the FY 2011 data in its FY 2012 IPERA audit report. However, the auditors discussed this matter in the body of the report.

On September 16, 2013, the QA Manager reported that although the auditors discussed that they did not validate the accuracy and completeness of the data in the body of the report, the auditors omitted this fact from Appendix A, Scope and Methodology. The AIGA did not specifically address the omission in the September 4, 2013 response to the QA report.

For the FY 2013 IPERA audit, the auditors did not report, in the scope paragraph, the following as limitations due to:

- three Government agencies failure to confirm payments made on behalf of DIA;
- DIA's inability to access the Department of Treasury's Do Not Pay Database as required by Section 5 of Public Law 112-248, "Improper Payments Elimination and Recovery Improvement Act of 2012" January 10, 2013;
- time constraints for reporting on the program and the reason the auditors gave for limiting their sample size; and
- the exclusion of the Civilian Pay and Travel Programs from the DIA universe of susceptible programs subject to significant improper payment.

The user of the audit report could be misled if the auditors do not report scope limitations in the Audit Scope and Methodology section of the audit report. Specifically, the user could be misled if the auditors do not report conditions or events that did not allow them to accomplish planned procedures such as confirming third party payments from service providers.

## Relationship Between the Population and the Items Tested Not Reported

For the FY 2013 IPERA audit, the auditors did not report the relationship between the 40 transactions tested and the population and did not report the monetary value of the sample size to the population. GAGAS 7.12 states in describing the work conducted to address the audit objectives and support the reported findings and conclusions, auditors should, as applicable, explain the relationship between the population and the items tested; identify organizations, geographic locations, and the period covered; report the kinds and sources of evidence; and explain any significant limitations or uncertainties based on the auditors' overall assessment of the sufficiency and appropriateness of the evidence in the aggregate. The Audit Division's Audit Handbook Chapter 4, "Reporting, Scope, Universe," states that the team should describe the universe – what was available for sample selection. As appropriate, this should include both dollar value and number of items in the universe. Because the auditors did not report on the population, the users of the report do not have enough information on the sufficiency of testing and evidence examined in this audit.

## Extent of Work Performed Not In Perspective

For the three audits reviewed, the use of computer processed data was not placed in perspective when used to support conclusions. GAGAS 7.16 states auditors should place their findings in perspective by describing the nature and extent of the issues being reported and the extent of the work performed that resulted in the finding. The DIA OIG Audit Division's Audit Handbook, "Chapter 4, "Reporting, Scope, Computer-processed Data," provides if the team's findings, conclusions, or recommendations are based on or derived from computer-processed data, the scope of the report must discuss whether or not the data were sufficient and appropriate.

- For the CERP audit, DIA OIG, Audit Division reported that the auditors did not find any discrepancies in the data for the contract actions and funding documents reviewed. However, on the referenced working paper the auditors documented, in part in the conclusion, that the review of system controls and the results of data tests showed incomplete data records with missing data attributes. The information reported is inconsistent with the audit documentation used to support the conclusion in the report.

- For the FY 2012 IPERA audit, the auditors did not report on FY 2012 payments as stated in the second objective of the report. Instead, the auditors reported on the FY 2011 payments from DIA's baseline report dated September 30, 2012. The auditors reported as if the payments were made in FY 2012. In reporting, the auditors did not immediately attribute the payments to FY 2011. The auditors mentioned FY 2011 twice in the entire report once in the "Background and Criteria" section and again in the "Programs Required Improper Payments Information" section of the report. The user of the report would need access to both reports to determine that the amounts reported came from the report dated September 30, 2012.
- For the FY 2013 IPERA audit, contrary to what the auditors reported, computer-processed data materially supported conclusions. The auditors identified errors in the payment information that DIA reported for two programs. The errors resulted in the overstatement of payments on one program and underpayments on another program. The auditors also used computer processed data to report on FY 2013 DIA payments.

The user of the audit reports could be misled if reported information is not kept in perspective. However, we did not determine that the deficiencies affected the findings and recommendations reported.

### *Conflicts Between the Audit Report Statement and Audit Documentation*

For all three audits reviewed, we identified instances when statements of fact were not always supported, not always supported on the referenced working paper, or not always referenced to the appropriate supporting documentation. However, the errors found did not impair the reliability of the findings and recommendations reported. GAGAS 7.27 states that auditors should report conclusions based on the audit objectives and the audit findings. Report conclusions are logical inferences about the program based on the auditors' findings, not merely a summary of the findings. The strength of the auditors' conclusions depends on the sufficiency and appropriateness of the evidence supporting the findings and the soundness of the logic used to formulate the conclusions. The Audit Division's Audit Handbook, Chapter 4, "Reporting, Independent Referencing Review, Audit Manager's Responsibility" states that the audit manager ensures that all statements of fact in the report have been fully referenced to the supporting project documentation and that the project documents have been adequately reviewed.

For the CERP audit, the units of equipment for May 2012 should be 2,208 based on the referenced working paper. In the Performance Work Statement Delivery Schedule, the auditors reported the units for the equipment ordered of 2,500. In addition, for the FY 2012 IPERA audit, in the "What We Did," "Audit Scope," and "Methodology" section of the report, the auditors' referenced audit procedures that they performed in the planning phase of the audit instead of procedures that they performed in the fieldwork phase of the audit. Finally, for the FY 2013 IPERA audit, the auditors reported on DIA's use of the improper payment rate for Defense Finance and Accounting Services for payment of DIA's Transactions by Others IPERA Program. The referenced working paper did not contain the improper payment rate on which the auditors reported for the Defense Finance and Accounting Services.

Errors identified in the report and referencing to non-supporting audit documentation for statements of fact in the report might cause knowledgeable third parties to question the reliability of the audit report.

## Quality Control Program

GAGAS 3.84 requires that each audit organization documents its quality control policies and procedures and communicate those policies and procedures to its personnel. The DIA OIG Audit Division established its quality control system in its Audit Handbook. GAGAS 3.93 states that the purpose of monitoring compliance with quality control policies and procedures is to provide an evaluation of whether the:

- professional standards and legal and regulatory requirements have been followed,
- quality control system has been appropriately designed, and
- quality control policies and procedures are operating effectively and complied with in practice.

In three audits, the Audit Division's staff did not determine whether quality control policies and procedures were operating effectively and complied with in practice. As a result, we identified the following areas for improvement in DIA OIG Audit Division's system of quality control:

- completing the quality control checklist for management review;
- completing quality control checklist throughout the audit; and
- determining the appropriateness of answers on checklists for DIA OIG Audit Division's audit staff to increase compliance with GAGAS.

## Completing Quality Control Checklist for Management Review

For the three audits reviewed, the AIGA did not complete the "Quality Control Checklist for Management Review – AIGA/DAIGA" (Assistant Inspector General for Audit/Deputy Assistant Inspector General for Audit). The Audit Division's Audit Handbook Section 1.4, "Quality Control and Assurance, Quality Control Program, Assistant Inspector General for Audits" requires the AIGA to conduct periodic quality control reviews of each project to ensure they meet GAGAS and Audit Handbook procedures.

## Completing of Quality Control Checklists throughout the Audit

For all three audits reviewed, the auditors did not document completion of the "Quality Control Checklist" throughout the audit. The Audit Division's Audit Handbook Chapter 1, "General Standards," Section 1.4, "Quality Control and Assurance, Quality Control Program, Project Reviews/Certifications," provides that each level of Audit Leadership is responsible for following their respective, "Quality Control Checklist," throughout the project to ensure the execution of quality, timely, and relevant projects. As a result of not completing the required checklists, the auditors did not determine whether the quality control policies and procedures operated effectively and that the auditors complied with the DIA OIG Audit Division's quality controls.

## Determining Appropriateness of Answers to Questions on the Checklists

For two of three audits, we identified instances when the audit team did not provide the appropriate answer to questions on the checklist. GAGAS paragraph 3.82 requires audit organizations to establish and maintain a system of quality control designed so the audit organization and its personnel comply with professional standards. DIA OIG's Audit Handbook, Chapter 1, Section 1.4, "General Standards, Quality Control and Assurance, Internal System of Quality Control" states, in part, that checklists are one input to the Audit Division's quality control services. The DIA OIG Audit Division's Audit Handbook established the system of quality control and states that checklists serve as inputs to the system of the quality control. DIA OIG Audit Division established this process to ensure audits have sufficient, appropriate evidence to support the findings and conclusion. For the FY 2013 IPERA audit the auditors answered "Yes" to the question "Did you express the effect in quantities (that is, amounts of potential monetary benefits, units of production) if possible? "Not Applicable" is the appropriate answer because the Audit Division did not report on potential monetary benefits.

On September 16, 2013, and May 28, 2014, the QA Manager reported similar concerns for improving the quality control system. Regarding the completion of the "Quality Control Checklist for Management Review – AIGA/DAIGA" the AIGA responded to making a concerted effort to complete the checklist in future audits. For answering questions on the checklists, during this peer review, the AIGA responded that completing checklists is an area that could be strengthened. The AIGA also responded that the Audit Handbook and quality control checklists are being revised. According to the AIGA, the revisions will facilitate the evaluation of the work performed during the audit in a way that provides convincing evidence that the audit work meets the intent of the standards.

## Recommendations, Management Comments, and Our Response

### *Recommendation 1*

**We recommend that the Defense Intelligence Agency, Office of Inspector General, Assistant Inspector General for Audit appropriately implement a plan to include training, as necessary, to ensure auditors:**

- **Follow the generally accepted government auditing standards' Conceptual Framework approach to Independence.**
- **Evaluate data from information systems and determine what the component of the Defense Intelligence Agency did to obtain reliance on provided data.**
- **Assess the sufficiency and appropriateness of computer-processed information.**
- **Obtain an understanding of the internal controls significant to the audit objective.**
- **Obtain an understanding of the service provider agreements and contract terms, when applicable, and the nature and profile of programs being audited.**
- **Obtain assurance over the reliability of data provided by Defense Intelligence Agency officials and the methodology used by the officials to obtain their assurance in the data.**
- **Design and perform steps to detect fraud risk when it is likely to have occurred and to reduce audit risk to an acceptable level.**
- **Assess the objectivity, credibility, and reliability of testimonial evidence and corroborate testimonial evidence with documentary evidence when feasible.**
- **Ensure that reporting complies with the generally accepted government auditing standards reporting standards.**

### DIA OIG Comments

The Inspector General, DIA agreed with the recommendation. The Inspector General stated that on January 20, 2015, the AIGA updated, released, and communicated to the audit staff changes to the Audit Handbook. The AIGA updated the handbook using GAGAS requirements, as well as lessons learned from the peer review efforts. The updated Audit Handbook clearly outlines the GAGAS requirements, associated audit activities, and expected documentation of audit work related to the areas listed.

### Our Response

The DIA Inspector General's comments are responsive to the recommendation. No additional comments are needed.

## Recommendation 2

**We recommend that the Defense Intelligence Agency, Office of Inspector General, Assistant Inspector General for Audit reemphasize the policies and procedures governing the System of Quality Control to include how responses to checklists are used as a tool to help the auditors assess whether the audit complies with the generally accepted government auditing standards for general, fieldwork – planning; fieldwork – evidence, documentation and supervision; and reporting standards.**

### DIA OIG Comments

The Inspector General, DIA agreed with the recommendation. The DIA's Inspector General stated that the AIGA stressed to the audit staff through e-mail and at Division all-hands meetings the importance of the Audit Division system of quality control, as well as adherence to that system of quality control. The Inspector General also stated that on January 30, 2015, the AIGA and QA manager completed revisions to the audit project quality control checklists, posting the checklists on SharePoint and communicating the revisions to audit staff. Additionally, the Inspector General listed other corrective actions that the AIGA has taken based on quality assurance and peer review efforts to include implementing TeamMate audit software and increased monitoring of audit projects.

### Our Response:

DIA Inspector General's comments are responsive to the recommendation. No additional comments are needed.

# Appendix B

## Summary Results of Interviews

We interviewed five auditors, two audit managers, and the Assistant Inspector General for Audit at the DIA's headquarters to determine their knowledge of the DIA OIG Audit Division's audit policies and GAGAS general, fieldwork, and reporting standards. The following table contains a summary of the results of the responses received.

| Areas Pertaining to DIA OIG Audit Policies and GAGAS Standards | Staff Responses to Questions |
|---|---|
| Awareness of DIA OIG Audit Policies | The staff stated they were aware of the audit policies. |
| Compliance with GAGAS | The staff stated that their work complied with GAGAS. |
| Independence | The staff stated they are aware of the GAGAS Conceptual Framework and brainstorming requirements. |
| Competence | Staff responses indicated that they fulfilled the competency requirement. |
| Quality Control and Assurance | The staff was knowledgeable about quality control and assurance procedures. |
| Planning (Risk Assessments) | The staff stated that they completed risk assessments for their audits. |
| Supervision | The staff stated that they received (auditor) or provided (manager) adequate supervision. |
| Audit Documentation | The staff stated that the audit documentation was adequate. |
| Evidence | The staff stated that the evidence was adequate. |
| Reporting (Timeliness) | The staff stated that the reports were timely. |

# Appendix C

## Scope and Methodology

We reviewed the adequacy of the DIA OIG audit organization's compliance with its quality control policies, procedures, and GAGAS. In performing our review, we considered the requirements of quality control standards contained in the December 2011 Revision of GAGAS issued by the Comptroller General of the United States. GAGAS 3.96 states:

> The audit organization should obtain an external peer review at least once every 3 years that is sufficient in scope to provide a reasonable basis for determining whether, for the period under review, the reviewed audit organization's system of quality control was suitably designed and whether the audit organization is complying with its quality control system in order to provide the audit organization with reasonable assurance of conforming with applicable professional standards.

Similar requirements exist for the 2007 Version of GAGAS 3.50b, which we used to assess one terminated audit for compliance with GAGAS 7.49. We performed this review from August 2014 to November 2014 in accordance with standards and guidelines established in the March 2009, updated November 2012, CIGIE Guide for Conducting External Peer Reviews of the Audit Organizations of Federal Offices of Inspector General. We performed this review in accordance with CIGIE Quality Standards for Inspection and Evaluation. The National Security Agency, Office of Inspector General assigned an auditor to assist in this peer review from August 11, 2014 through September 12, 2014.

In performing this review, we assessed, reviewed, and evaluated audit documentation; interviewed DIA OIG audit staff and Audit Managers as well as the AIGA; reviewed DIA OIG Audit Division policies published on June 22, 2012, and updated on July 16, 2013. We also reviewed Quality Assurance reports pertaining to DIA OIG Audit Division's audit reports issued in FY 2013. Specifically, the QA Manager performed two technical and one quality assurance review during FY 2013. Of the three reviews performed two, a technical and quality control review, pertained to the FY 2012 IPERA audit, which we also reviewed.

We judgmentally selected three reports from a universe of four reports issued by the DIA OIG Audit Division's auditors from January 1, 2013 to April 30, 2014. Because DIA OIG Audit Division did not implement its quality control and assurance system until January 2013 we excluded reports issued for the periods ended December 31, 2011 and December 31, 2012 from our criteria. Additionally, we reviewed the September 16, 2013, report that the QA Manager issued to the Assistant Inspector General for Audit on the quality assurance review of the FY 2012 IPERA audit, and the memorandum dated May 28, 2014, for the results of two technical reviews and one quality assurance review.

Table C-1 identifies the specific reports reviewed. We obtained The Type of Review for the CERP audit from the report. Because the Audit Division did not identify the type of audit in the FY 2012 IPERA audit and the FY 2013 IPERA audit we obtained the Type of Review from DIA OIG Audit Division's listing of audit reports issued.

We assessed three of the four audit reports issued during the period January 1, 2013 through April 30, 2014, for compliance with the 2011 version of GAGAS. These audits began after the December 15, 2011, effective date of the 2011 version of the GAGAS and after the October 1, 2011 date scheduled for DIA OIG, Audit Division's implementation of its Quality Assurance Program to strengthen its Quality Control and Assurance System.

We also reviewed the only terminated audit for compliance with GAGAS 7.49, (2007 version). For the terminated Project 2011-100003, "DIA Compliance with OMB [Office Of Management and Budget] Guidance on Improving Government Acquisition" the Audit Division issued a memorandum, and terminated the audit on May 30, 2012, and reissued the termination memorandum on June 20, 2012. We reviewed the audit documentation for compliance with GAGAS 7.49 which states, in part, if an audit is terminated before it is completed and an audit report is not issued, auditors should document the results of the work to the date of termination and why the audit was terminated. The auditors communicated the reason for terminating the audit to the responsible DIA officials in two memorandums dated May 30, 2012 and June 20, 2012. The Audit Division re-announced Project 2011-100003-OA on October 6, 2011, before the December 15, 2011, effective date of the 2011 version of GAGAS. The auditors terminated the audit because the Department of Defense used a budget-based approach for complying with the Office of Management and Budget Guidance M-09-25, July 29, 2009.

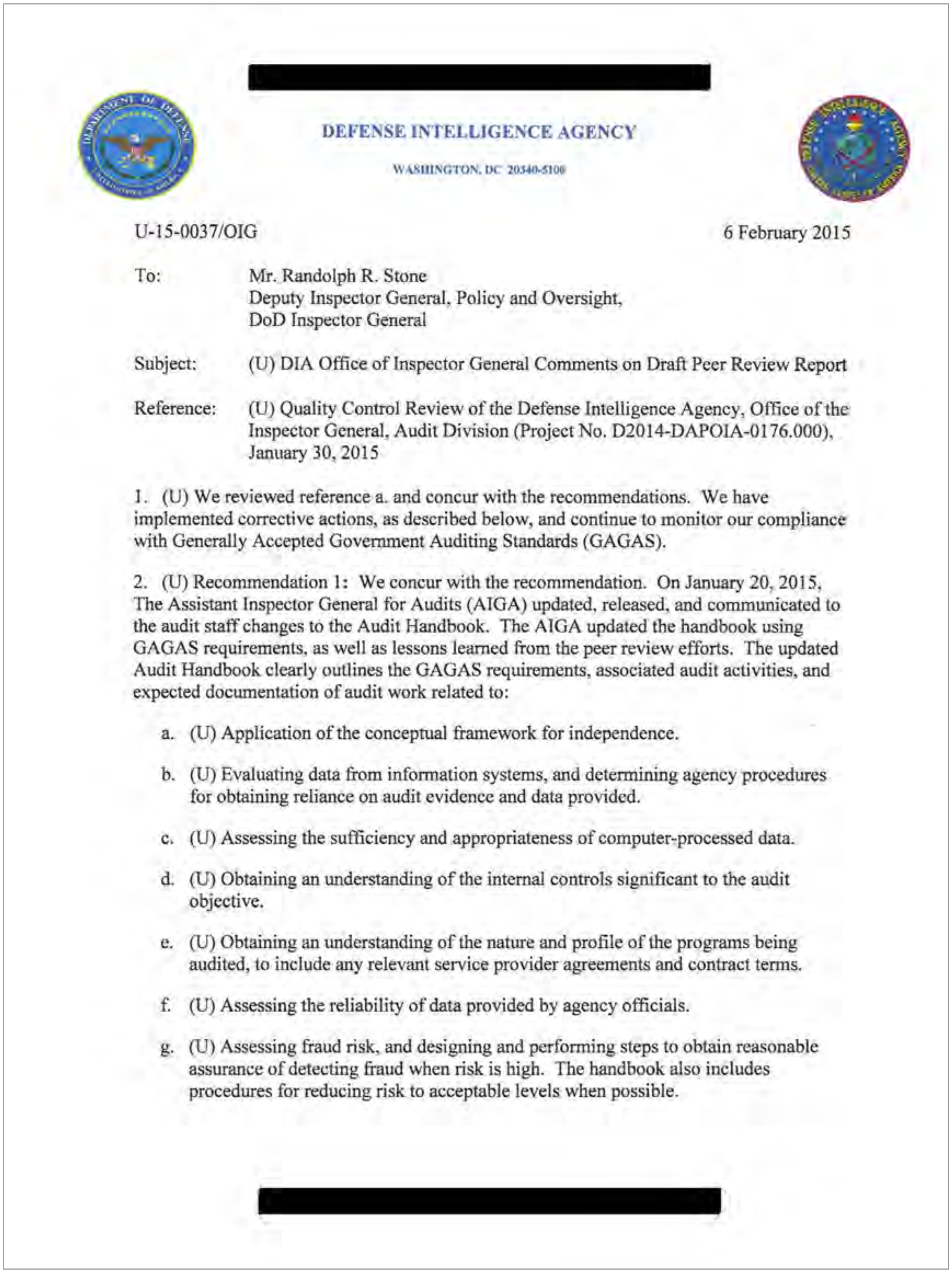
*Table C-1. Audits Reviewed*

| Project Number / Report Number | Report Title and Issue Date | Report Date | Type of Audit |
|---|---|---|---|
| 2011-100003-OA / U-12-0241/IG | DIA Compliance with OMB Guidance on Improving Government Acquisition | May 30, 2012 and June 20, 2012 | Terminated |
| 2012-100001-OA / U-13-0207/OIG | DIA's Capital Equipment Replacement Program (CERP) | June 17, 2013 | Performance |
| 2013-100001-OA / S-13-0078/IG | DIA's Compliance with the Improper Payments Elimination and Recovery Act of 2010 | March 15, 2013 | Performance |
| 2014-100000-OA / S-14-0116/OIG | DIA's Compliance with the Improper Payments Elimination and Recovery Act of 2010 | April 14, 2014 | Performance |

Our review would not necessarily disclose all weaknesses in the system of quality control or all instances of noncompliance because we based our review on selective tests. There are inherent limitations in considering the potential effectiveness of any quality control system. In performing most control procedures, departures can result from misunderstanding of instructions, mistakes of judgment, carelessness, or other human factors. Projecting any evaluation of a quality control system into the future is subject to the risk that one or more procedures may become inadequate because conditions may change or the degree of compliance with procedures may deteriorate.

# Management Comments

## Defense Intelligence Agency



[redacted]

DEFENSE INTELLIGENCE AGENCY

WASHINGTON, DC 20340-5100

U-15-0037/OIG

6 February 2015

To: Mr. Randolph R. Stone
Deputy Inspector General, Policy and Oversight,
DoD Inspector General

Subject: (U) DIA Office of Inspector General Comments on Draft Peer Review Report

Reference: (U) Quality Control Review of the Defense Intelligence Agency, Office of the Inspector General, Audit Division (Project No. D2014-DAPOIA-0176.000), January 30, 2015

1. (U) We reviewed reference a. and concur with the recommendations. We have implemented corrective actions, as described below, and continue to monitor our compliance with Generally Accepted Government Auditing Standards (GAGAS).

2. (U) Recommendation 1: We concur with the recommendation. On January 20, 2015, The Assistant Inspector General for Audits (AIGA) updated, released, and communicated to the audit staff changes to the Audit Handbook. The AIGA updated the handbook using GAGAS requirements, as well as lessons learned from the peer review efforts. The updated Audit Handbook clearly outlines the GAGAS requirements, associated audit activities, and expected documentation of audit work related to:

a. (U) Application of the conceptual framework for independence.

b. (U) Evaluating data from information systems, and determining agency procedures for obtaining reliance on audit evidence and data provided.

c. (U) Assessing the sufficiency and appropriateness of computer-processed data.

d. (U) Obtaining an understanding of the internal controls significant to the audit objective.

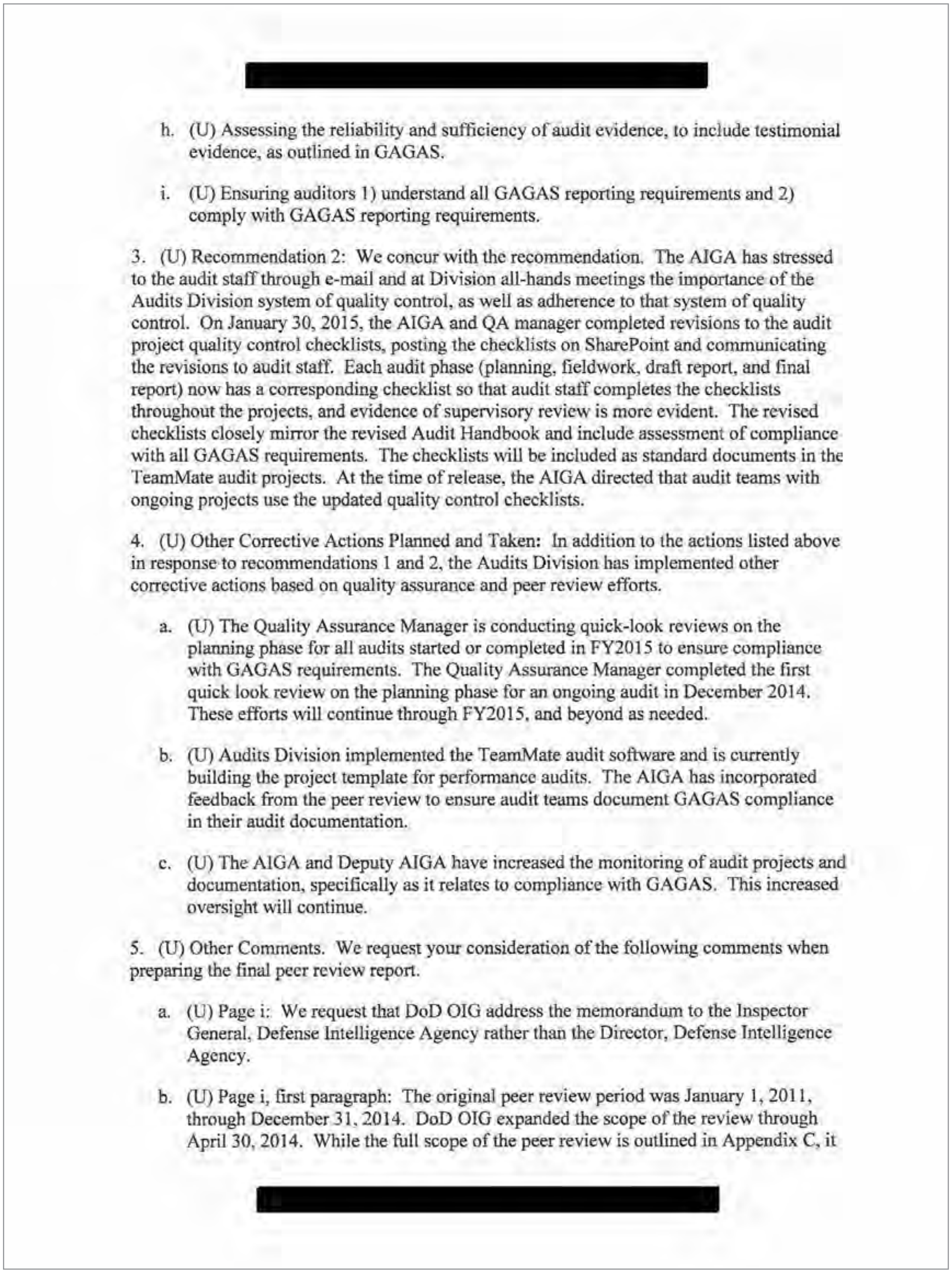
e. (U) Obtaining an understanding of the nature and profile of the programs being audited, to include any relevant service provider agreements and contract terms.

f. (U) Assessing the reliability of data provided by agency officials.

g. (U) Assessing fraud risk, and designing and performing steps to obtain reasonable assurance of detecting fraud when risk is high. The handbook also includes procedures for reducing risk to acceptable levels when possible.

[redacted]

## Defense Intelligence Agency (cont'd)



[redacted]

h. (U) Assessing the reliability and sufficiency of audit evidence, to include testimonial evidence, as outlined in GAGAS.

i. (U) Ensuring auditors 1) understand all GAGAS reporting requirements and 2) comply with GAGAS reporting requirements.

3. (U) Recommendation 2: We concur with the recommendation. The AIGA has stressed to the audit staff through e-mail and at Division all-hands meetings the importance of the Audits Division system of quality control, as well as adherence to that system of quality control. On January 30, 2015, the AIGA and QA manager completed revisions to the audit project quality control checklists, posting the checklists on SharePoint and communicating the revisions to audit staff. Each audit phase (planning, fieldwork, draft report, and final report) now has a corresponding checklist so that audit staff completes the checklists throughout the projects, and evidence of supervisory review is more evident. The revised checklists closely mirror the revised Audit Handbook and include assessment of compliance with all GAGAS requirements. The checklists will be included as standard documents in the TeamMate audit projects. At the time of release, the AIGA directed that audit teams with ongoing projects use the updated quality control checklists.

4. (U) Other Corrective Actions Planned and Taken: In addition to the actions listed above in response to recommendations 1 and 2, the Audits Division has implemented other corrective actions based on quality assurance and peer review efforts.

a. (U) The Quality Assurance Manager is conducting quick-look reviews on the planning phase for all audits started or completed in FY2015 to ensure compliance with GAGAS requirements. The Quality Assurance Manager completed the first quick look review on the planning phase for an ongoing audit in December 2014. These efforts will continue through FY2015, and beyond as needed.

b. (U) Audits Division implemented the TeamMate audit software and is currently building the project template for performance audits. The AIGA has incorporated feedback from the peer review to ensure audit teams document GAGAS compliance in their audit documentation.

c. (U) The AIGA and Deputy AIGA have increased the monitoring of audit projects and documentation, specifically as it relates to compliance with GAGAS. This increased oversight will continue.

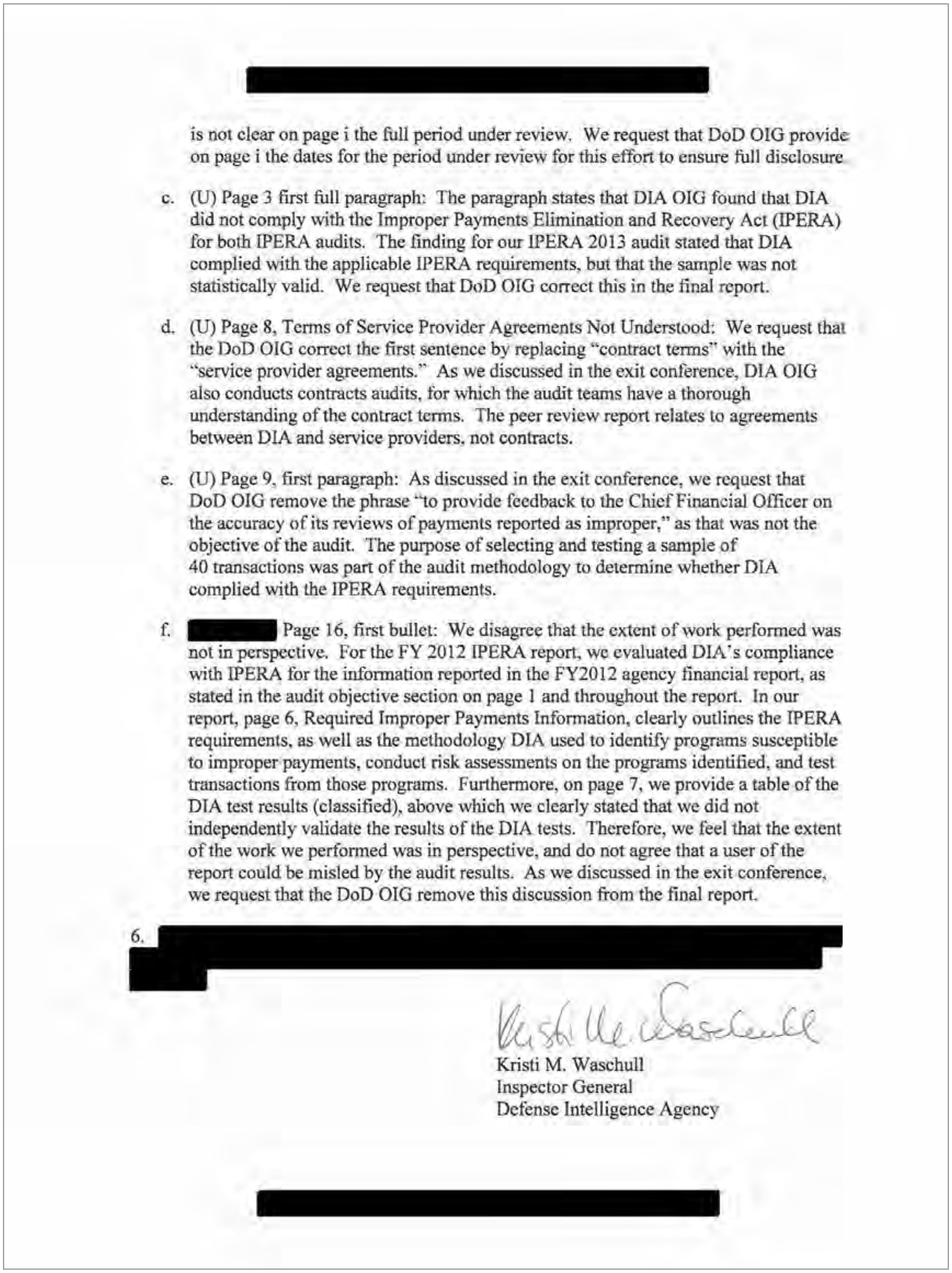
5. (U) Other Comments. We request your consideration of the following comments when preparing the final peer review report.

a. (U) Page i: We request that DoD OIG address the memorandum to the Inspector General, Defense Intelligence Agency rather than the Director, Defense Intelligence Agency.

b. (U) Page i, first paragraph: The original peer review period was January 1, 2011, through December 31, 2014. DoD OIG expanded the scope of the review through April 30, 2014. While the full scope of the peer review is outlined in Appendix C, it

[redacted]

## Defense Intelligence Agency (cont'd)



[redacted]

is not clear on page i the full period under review. We request that DoD OIG provide on page i the dates for the period under review for this effort to ensure full disclosure

c. (U) Page 3 first full paragraph: The paragraph states that DIA OIG found that DIA did not comply with the Improper Payments Elimination and Recovery Act (IPERA) for both IPERA audits. The finding for our IPERA 2013 audit stated that DIA complied with the applicable IPERA requirements, but that the sample was not statistically valid. We request that DoD OIG correct this in the final report.

d. (U) Page 8, Terms of Service Provider Agreements Not Understood: We request that the DoD OIG correct the first sentence by replacing "contract terms" with the "service provider agreements." As we discussed in the exit conference, DIA OIG also conducts contracts audits, for which the audit teams have a thorough understanding of the contract terms. The peer review report relates to agreements between DIA and service providers, not contracts.

e. (U) Page 9, first paragraph: As discussed in the exit conference, we request that DoD OIG remove the phrase "to provide feedback to the Chief Financial Officer on the accuracy of its reviews of payments reported as improper," as that was not the objective of the audit. The purpose of selecting and testing a sample of 40 transactions was part of the audit methodology to determine whether DIA complied with the IPERA requirements.

f. [redacted] Page 16, first bullet: We disagree that the extent of work performed was not in perspective. For the FY 2012 IPERA report, we evaluated DIA's compliance with IPERA for the information reported in the FY2012 agency financial report, as stated in the audit objective section on page 1 and throughout the report. In our report, page 6, Required Improper Payments Information, clearly outlines the IPERA requirements, as well as the methodology DIA used to identify programs susceptible to improper payments, conduct risk assessments on the programs identified, and test transactions from those programs. Furthermore, on page 7, we provide a table of the DIA test results (classified), above which we clearly stated that we did not independently validate the results of the DIA tests. Therefore, we feel that the extent of the work we performed was in perspective, and do not agree that a user of the report could be misled by the audit results. As we discussed in the exit conference, we request that the DoD OIG remove this discussion from the final report.

6. [redacted]

Kristi M. Waschull
Inspector General
Defense Intelligence Agency

[redacted]

# Acronyms and Abbreviations

| | |
|---|---|
| **AIGA** | Assistant Inspector General for Audit |
| **DIA** | Defense Intelligence Agency |
| **FACTS** | Financial Accounting and Corporate Tracking System |
| **GAGAS** | Generally Accepted Government Auditing Standards |
| **IPERA** | Improper Payments Elimination and Recovery Act of 2010 |
| **OIG** | Office of the Inspector General |
| **OMB** | Office of Management and Budget |

## Whistleblower Protection

### U.S. Department of Defense

*The Whistleblower Protection Enhancement Act of 2012 requires the Inspector General to designate a Whistleblower Protection Ombudsman to educate agency employees about prohibitions on retaliation, and rights and remedies against retaliation for protected disclosures. The designated ombudsman is the DoD Hotline Director. For more information on your rights and remedies against retaliation, visit www.dodig.mil/programs/whistleblower.*

## For more information about DoD IG reports or activities, please contact us:

**Congressional Liaison**
congressional@dodig.mil; 703.604.8324

**Media Contact**
public.affairs@dodig.mil; 703.604.8324

**Monthly Update**
dodigconnect-request@listserve.com

**Reports Mailing List**
dodig_report@listserve.com

**Twitter**
twitter.com/DoD_IG

**DoD Hotline**
dodig.mil/hotline

DEPARTMENT OF DEFENSE | INSPECTOR GENERAL

4800 Mark Center Drive
Alexandria, VA 22350-1500
www.dodig.mil
Defense Hotline 1.800.424.9098