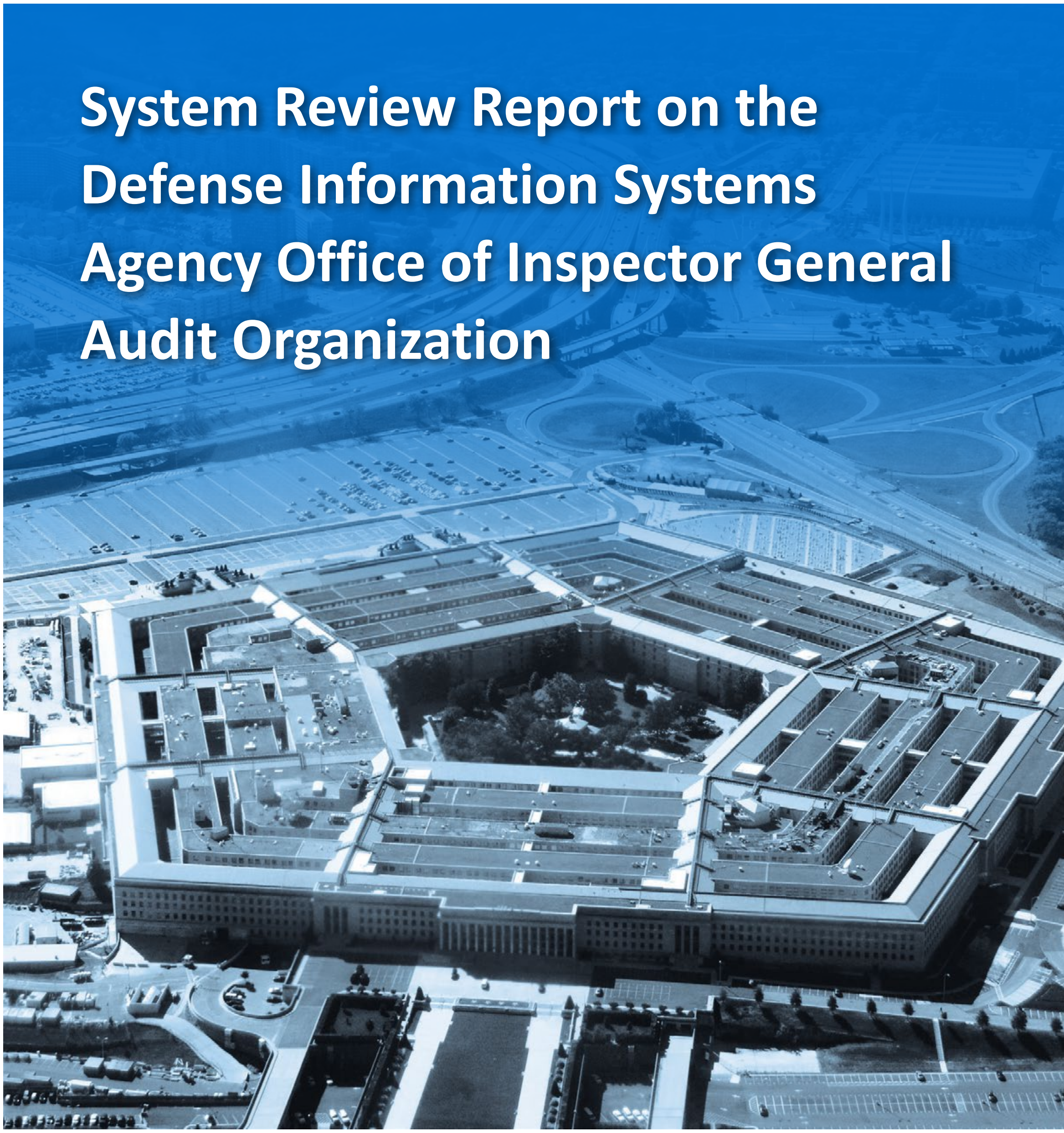
Report No. DODIG-2021-031

INSPECTOR GENERAL

U.S. Department of Defense

DECEMBER 9, 2020



System Review Report on the Defense Information Systems Agency Office of Inspector General Audit Organization

INTEGRITY ★ INDEPENDENCE ★ EXCELLENCE

INSPECTOR GENERAL

INTEGRITY EFFICIENCY

DEPARTMENT OF DEFENSE

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

December 9, 2020

MEMORANDUM FOR DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY

SUBJECT: System Review Report on the Defense Information Systems Agency Office of Inspector General Audit Organization (Report No. DODIG-2021-031)

The final report provides the results of the DoD Office of Inspector General's peer review on the Defense Information Systems Agency Office of Inspector General audit organization. We previously provided copies of the draft report and requested written comments on the recommendations. We considered management's comments on the draft report when preparing the final report. These comments are included in Enclosure 2 of the report.

The Defense Information Systems Agency Inspector General agreed to, and addressed, all the recommendations presented in the report. Comments from the Defense Information Systems Agency conformed to the requirements of DoD Instruction 7650.03; therefore, we do not require additional comments.

If you have any questions or would like to meet to discuss the peer review, please contact [redacted] We appreciate the cooperation and assistance we received during the peer review.

Randolph R. Stone
Assistant Inspector General for Evaluations
Space, Intelligence, Engineering, and Oversight

INSPECTOR GENERAL

INTEGRITY EFFICIENCY

DEPARTMENT OF DEFENSE

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

December 9, 2020

MEMORANDUM FOR DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY

SUBJECT: System Review Report on the Defense Information Systems Agency Office of Inspector General Audit Organization (Report No. DODIG-2021-031)

We reviewed the system of quality control for the Defense Information Systems Agency (DISA) Office of the Inspector General (OIG) audit organization in effect for the 3-year period ended May 31, 2020. A system of quality control encompasses the DISA OIG audit organization's structure, the policies adopted, and procedures established to provide it with reasonable assurance of conforming in all material respects with the *Government Auditing Standards* and applicable legal and regulatory requirements. The elements of quality control are described in the *Government Auditing Standards*.

In our opinion, the system of quality control for the DISA OIG audit organization in effect for the 3-year period ended May 31, 2020, has been suitably designed and complied with to provide the DISA OIG audit organization with reasonable assurance of performing and reporting in conformity in all material respects with applicable professional standards.

Audit organizations can receive a rating of *pass*, *pass with deficiencies*, or *fail*. The DISA OIG audit organization has received a rating of *pass*.

Letter of Comment

We have issued a Letter of Comment dated December 9, 2020, that sets forth findings we did not consider to be of sufficient significance to affect our opinion expressed in this report.

Basis of Opinion

We conducted our review in accordance with the *Government Auditing Standards* and the Council of the Inspectors General on Integrity and Efficiency *Guide for Conducting Peer Reviews of the Audit Organizations of Federal Offices of Inspector General*, March 2020.

During our review, we interviewed DISA OIG audit personnel and obtained an understanding of the nature of the DISA OIG audit organization and the design of its system of quality control sufficient to assess the risks implicit in its audit function. Based on our assessment, we selected three of eight performance audits that DISA OIG completed and the one audit that DISA OIG terminated between December 22, 2017, and April 30, 2020. We tested the four audits for conformity with the *Government Auditing Standards*. The four audits we selected represent a reasonable cross-section of the universe of nine audits performed by the DISA OIG audit organization during the 3-year period ended May 31, 2020.

In performing our review, we obtained an understanding of the system of quality control for the DISA OIG audit organization. In addition, we tested for compliance with the DISA OIG audit organization's quality control policies and procedures to the extent that we considered appropriate. These tests covered the application of the DISA OIG audit organization's policies and procedures on the selected audits. Our review was based on selected tests; therefore, it would not necessarily detect all weaknesses in the system of quality control or all instances of noncompliance with it.

We met with the DISA OIG audit organization's management to discuss the results of our review. We believe that the procedures we performed provide a reasonable basis for our opinion. Enclosure 1 identifies the scope and methodology, the DISA OIG audit offices we visited during this review (see Table 1), and the four audits we reviewed.

Responsibilities and Limitation

The DISA OIG audit organization is responsible for establishing and maintaining a system of quality control designed to provide the DISA OIG with reasonable assurance that the organization and its personnel comply in all material respects with professional standards and applicable legal and regulatory requirements. Our responsibility is to express an opinion on the design of the system of quality control and the DISA OIG audit organization's compliance based on our review.

There are inherent limitations in the effectiveness of any system of quality control; therefore, noncompliance with the system of quality control may occur and not be detected. Projection of any evaluation of a system of quality control to future periods is subject to the risk that the system of quality control may become inadequate because of changes in conditions or because the degree of compliance with the policies or procedures may deteriorate.

Randolph R. Stone
Assistant Inspector General for Evaluations
Space, Intelligence, Engineering, and Oversight

Enclosures
As stated

Enclosure 1

Scope and Methodology

We conducted this peer review from June 2020 through October 2020 in accordance with the *Government Auditing Standards* and the Council of the Inspectors General on Integrity and Efficiency (CIGIE) *Guide for Conducting Peer Reviews of the Audit Organizations of Federal Offices of Inspector General*. These standards require that we obtain an understanding of the audit organization's system of quality control and conclude whether the:

- system is designed appropriately to ensure compliance with the *Government Auditing Standards*, and
- audit organization is complying with the *Government Auditing Standards* and internal policies and procedures.

Table 1 shows the DISA OIG audit organizational structure and locations for the headquarters and two field offices.

Table 1. DISA OIG Audit Organizational Structure and Locations

Audit Organizational Structure	Location
Headquarters	Fort Meade, Maryland
Field Offices:	
DISA OIG Audit Office	Columbus, Ohio
DISA OIG Audit Office	Scott Air Force Base, Illinois

Source: The DISA OIG.

This peer review covered the 3-year period from June 1, 2017, through May 31, 2020. We tested compliance with the DISA OIG audit organization system of quality control to the extent we considered appropriate. These tests included a review of four non-statistically selected projects, comprising three of eight performance audits and the one terminated audit, conducted by the DISA OIG audit organization from June 1, 2017, through May 31, 2020. We used the appendixes and procedures in the March 2020 CIGIE Guide identified in the following sections to conduct this external peer review.

Policies and Procedures (CIGIE Guide Appendix A)

We reviewed the DISA OIG audit policies and procedures to determine whether the policies and procedures complied with the *Government Auditing Standards*, including the American Institute of Certified Public Accountants Statements on Standards for Attestation Engagements, which is incorporated in the *Government Auditing Standards* by reference. We requested that the DISA OIG complete Column 1 of CIGIE Guide Appendix A, "Policies and Procedures," and provide a copy of relevant policies and procedures. In Column 2 of CIGIE Guide Appendix A, we recorded our conclusions and comments on the DISA OIG policies and procedures compliance with the *Government Auditing Standards*.

Checklist for the Standards of Independence, Competence and Continuing Professional Education, and Quality Control and Peer Review (CIGIE Guide Appendix B)

Using the CIGIE Guide's Appendix B, we tested the DISA OIG audit organization's compliance with the *Government Auditing Standards'* general standards, consisting of independence, competence, continuing professional education, and quality control and assurance. We reviewed the continuing professional education documentation for 13 of 18 audit staff members to determine whether they obtained the required number of continuing professional education hours and to determine whether the staff members were competent.[1] We also reviewed documentation of independence to determine whether the DISA OIG audit organization met the *Government Auditing Standards'* requirements for independence documentation.

Additionally, we reviewed all three of the DISA OIG internal quality assurance reviews completed from June 1, 2017, through May 31, 2020, to determine whether the audit organization:

- performed monitoring procedures that enabled it to assess compliance with professional standards, as well as quality control policies and procedures; and furthermore,
- analyzed and summarized the results of its monitoring procedures, at least annually, with identification of any systemic or repetitive issues needing improvement with recommendations for corrective action.

Checklist for Performance Audits Performed by the Office of Inspector General (CIGIE Guide Appendix E)

From June 1, 2017, through May 31, 2020, the DISA OIG audit organization completed eight performance audits. We non-statistically selected three performance audits for review. In selecting our non-statistical sample, we chose projects that would provide a reasonable cross-section of projects completed by the DISA OIG audit organization. For example, we chose projects that resulted in the selection of various DISA OIG managers and audit staff members. Using the CIGIE Guide's Appendix E, we reviewed the three performance audits to determine the extent to which the audits complied with the *Government Auditing Standards*.

The three performance audits we reviewed were conducted while the December 2011 revision to the *Government Auditing Standards* was in effect. Our recommendations in the Letter of Comment reference the July 2018 revision of the *Government Auditing Standards* because the July 2018 revision applies for performance audits beginning on or after July 1, 2019. Table 2 lists the audits we selected for review.

[1] We did not review the continuing professional education documentation for five audit staff members because they began working within the DISA OIG audit organization after the reviewed 2-year continuing professional education cycle which covered FY 2017 through FY 2018.

Table 2. DISA OIG Audits Selected

Title	Project Number	Type of Audit
Audit of the DISA Global Service Desk	18_IG2_005_600_AA	Performance Audit
Audit of DISA's Contractor Workspace Management	19_IG2_001_300_AA	Performance Audit
Audit of DISA's Compliance with Contracting Requirements for Cyber Safeguards of Covered Defense Information	16_IG21_004_300_AA	Performance Audit

Source: The DoD OIG.

Terminated Audit (CIGIE Risk Assessment Procedure)

The DISA OIG audit organization's universe of audits from June 1, 2017, through May 31, 2020, included one audit that was terminated. We reviewed the audit documentation for the terminated audit, "Audit of Controls Over Contract Security Classification Specification (DD Form 254)," Project No. 16_IG21_001_400_AA, to determine whether the DISA OIG audit staff documented the results of the work to the date of termination and the reason they terminated the audit.

Audit Staff Interviews (CIGIE Risk Assessment Procedure)

We interviewed 13 of the 18 the audit staff members at the three DISA OIG audit offices to determine whether DISA OIG audit management communicated quality control policies and procedures to the audit staff members.[2] We also assessed the audit staff members' understanding of, and compliance with, the DISA OIG quality control policies and procedures.

Use of Computer-Processed Data

We did not use computer-processed data to perform this external peer review.

Prior Coverage

During the last five years, the DoD OIG issued one report discussing the external peer review of the DISA OIG audit organization. Unrestricted DoD OIG reports can be accessed at www.dodig.mil/reports.

DoD OIG

Report No. DODIG-2018-001, "External Peer Review Report on the Defense Information Systems Agency, Office of Inspector General Audit Organization," October 12, 2017

> The DoD OIG evaluated whether the DISA OIG audit organization's system of quality control in effect for the 3-year period ended May 31, 2017, was suitably designed and whether the DISA OIG audit organization complied with its quality control system to provide it with reasonable assurance of conformity with the applicable professional standards.

[2] We did not interview five audit staff members within the DISA OIG audit organization because one staff member retired 1 month before we conducted the interviews, one staff member is an analyst, and three staff members provided audit liaison support and did not perform audits.

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

December 9, 2020

MEMORANDUM FOR DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY

SUBJECT: Letter of Comment on the External Peer Review of the DISA OIG Audit Organization (Report No. DODIG-2021-031)

We have reviewed the system of quality control for the Defense Information Systems Agency (DISA) Office of the Inspector General (OIG) audit organization in effect for the 3-year period ended May 31, 2020, and have issued our System Review Report on December 9, 2020, in which the DISA OIG audit organization received a rating of *pass*. The findings in this Letter of Comment should be read in conjunction with the System Review Report. The findings described below were not considered to be of sufficient significance to affect the opinion expressed in the System Review Report.

Finding 1. The Defense Information Systems Agency Office of Inspector General Audit Handbook Does Not Contain Policies and Procedures in Three Areas Pertaining to Fieldwork and Reporting Standards

The DISA OIG Audit Handbook does not contain policies and procedures in three areas pertaining to fieldwork and reporting standards for all engagements. *Government Auditing Standards* (GAS) 5.02 states an audit organization conducting engagements in accordance with the *Government Auditing Standards* must establish and maintain a system of quality control that is designed to provide the audit organization with reasonable assurance that the organization and its personnel comply with professional standards and applicable legal and regulatory requirements.

The DISA OIG Audit Handbook does not contain policies and procedures for the following three areas.

- GAS 5.24a states the audit organization should establish policies and procedures designed to provide it with reasonable assurance that appropriate consultation takes place on difficult or contentious issues that arise among engagement team members in the course of conducting a GAS engagement.

- GAS 7.56 and 9.51 state that when the responsible officials provide oral comments only, auditors should prepare a summary of the oral comments, provide a copy of the summary to the responsible officials to verify that the comments are accurately represented, and include the summary in their report.[3]
- GAS 7.58 and 9.53 state if the audited entity refuses to provide comments or is unable to provide comments within a reasonable period of time, the auditors should issue the report without receiving comments from the audited entity. In such cases, the auditors should indicate in the report that the audited entity did not provide comments.[4]

Recommendation, Management Comments, and Our Response

Recommendation 1

We recommend that the Defense Information Systems Agency Inspector General update the Audit Handbook to include policies and procedures that address the following three areas:

a. Consulting and documenting difficult or contentious issues that arise among audit team members during the engagement and the parties' understanding of the resulting conclusions reached and implemented.

b. Providing a summary of any management comments received only in oral form to responsible officials and including a summary of the comments in the report.

c. Stating in the report that the audited entity did not provide comments if the audited entity refuses to provide comments or is unable to provide comments within a reasonable period of time.

Defense Information Systems Agency Inspector General Comments

The DISA Inspector General agreed with the recommendation and stated the DISA OIG Audit Handbook was updated in November 2020 to include policies and procedures that address *Government Auditing Standards* sections 5.24a, 7.56, 9.51, 7.58, and 9.53. In addition, the DISA OIG audit staff were provided training on the updates in November 2020.

Our Response

Comments from the DISA Inspector General addressed all specifics of the recommendation. We reviewed the DISA OIG Audit Handbook and verified the updated policies and procedures. In addition, we verified that the DISA OIG audit staff was provided training on the updates in November 2020. Therefore, the recommendation is closed.

[3] GAS 7.56 is the standard for attestation engagements and reviews of financial statements and GAS 9.51 is the standard for performance audits.

[4] GAS 7.58 is the standard for attestation engagements and reviews of financial statements and GAS 9.53 is the standard for performance audits.

Finding 2. A Defense Information System Agency Office of Inspector General Audit Report Did Not Explain the Relationship Between the Task Orders Reported on and the Contract Awards Sampled

For one of the three DISA OIG audit reports we reviewed, the audit report did not explain the relationship between the task orders reported on and the contract awards sampled. Specifically, Finding A of the audit report for the, "Audit of DISA's Compliance with Contracting Requirements for Cyber Safeguards of Covered Defense Information," did not explain the relationship between 24 task orders reported on and the 90 information technology (IT) service contract awards sampled.[5]

GAS 7.11 states auditors should describe the scope of the work performed that would be relevant to likely users, so that they could reasonably interpret the findings and conclusions in the report. Also, GAS 7.12 states that 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. Further, GAS 7.13 states that in reporting audit methodology, auditors should explain how the completed audit work supports the audit objectives, including the evidence gathering and analysis techniques, in sufficient detail to allow knowledgeable users of their reports to understand how the auditors addressed the audit objectives.[6]

The objective of the audit was to determine whether DISA's IT service contracts contained required Defense Federal Acquisition Regulation Supplement (DFARS) contract clause 252.204-7012. The DISA OIG selected a sample of 90 IT service contract awards over $5,000 for testing, consisting of 45 base contracts and purchase orders and 45 task orders.

Finding A of the audit report stated "Fifty percent, 12 of 24, of the DISA task orders awarded from the GSA [General Services Administration] contracts tested did not include DFARS contract clause 252.204-7012." However, the audit report did not clearly explain whether or not the 24 GSA task orders were among the 90 IT service contracts awards (including 45 task orders) that DISA selected for testing. Finding A only reported on the results for the 24 GSA task orders tested, not on the results for all 90 IT service contracts sampled.

[5] Report No. 16_IG21_004_300_AA, "Audit of DISA's Compliance with Contracting Requirements for Cyber Safeguards of Covered Defense Information," September 27, 2018.

[6] The DISA OIG audit organization conducted the "Audit of DISA's Compliance with Contracting Requirements for Cyber Safeguards of Covered Defense Information" (Report No. 16_IG21_004_300_AA) under the December 2011 GAS revision. The requirements in GAS 7.11, GAS 7.12 and GAS 7.13 of the 2011 GAS revision were moved to sections 9.12, 9.13 and 9.14, respectively, of the July 2018 GAS revision.

The DISA OIG auditors informed us that the 24 GSA task orders were among the 90 IT service contracts awards that were selected for testing. The DISA auditors also stated that the 24 GSA task orders were part of a sub-population of task orders identified as high-risk of not including the DFARS contract clause.[7] The DISA OIG auditors further explained that the audit report focused on the 24 task orders awarded from the GSA contracts because these were the only type of task order found to have not included the DFARS contract clause.

Based on our review of the DISA working papers for the audit, we confirmed that the 24 GSA task orders were among the 90 service contracts awards selected for testing. Explaining in the audit report the relationship between the 24 GSA task orders reported on and the 90 IT service contract awards selected for testing would have been useful to fully describe the work performed that supported the reported findings and conclusions, and to help report users reasonably interpret the findings and conclusions.

Recommendation, Management Comments, and Our Response

Recommendation 2

We recommend that the Defense Information Systems Agency Inspector General issue a memorandum to the audit staff to emphasize that auditors must explain the scope of work performed in the audit report, including the relationship between items reported on and the items sampled, in accordance with the 2018 revision of Government Auditing Standard 9.12, 9.13, and 9.14.

Defense Information Systems Agency Inspector General Comments

The DISA Inspector General agreed with the recommendation. In November 2020, the Chief, Audit and Liaison Division issued a memorandum to the DISA OIG audit staff that reinforced the requirement to explain the scope of work performed in the audit report, including the relationship between items reported on and items sampled.

Our Response

Comments from the DISA Inspector General addressed all specifics of the recommendation. We verified that the November 2020 memorandum issued to the DISA OIG auditors reinforced the requirement to explain the scope of work performed in the audit report, including the relationship between items reported on and the items sampled. Therefore, the recommendation is closed.

[7] Third party task orders were also awarded from U.S. Department of Health and Human Services, Naval Supply Systems Command, National Aeronautics and Space Administration, and White House Communications Agency contracts.

Finding 3. The Project File for an Audit Terminated in December 2017 Did Not Include an Explanation for Why the Audit Was Terminated Until March 2019

The project file for Project No. 16_IG21_001_400_AA, "Audit of Controls Over Contract Security Classification Specification (DD Form 254)," the only audit that the DISA OIG terminated, did not include an explanation for why the audit was terminated until March 2019. The explanation for the termination was added to the project file 15 months after the DISA OIG terminated the audit in December 2017. GAS 6.50 states that if an engagement 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 engagement was terminated.[8]

In March 2019, the Chief of the Audit and Liaison Division reviewed the project file after the Branch Chief departed the agency, and found that the termination documentation was not included. As a result, an explanation of the termination was added to the project file at that time.

The *Government Auditing Standards* do not specify a timeframe for when auditors should prepare documentation stating why an audit was terminated. However, preparing the justification documentation when the decision is made to terminate the audit is a good practice that the DISA OIG audit organization should implement. Personnel changes, such as an audit staff member leaving the DISA OIG, may preclude audit personnel from having the necessary historical knowledge to create the documentation at a later date.

Recommendation, Management Comments, and Our Response

Recommendation 3

We recommend that the Defense Information Systems Agency Inspector General create a control, such as a checklist, for terminated audits. The control should include a step to verify that documentation to explain the reason for the termination is included in the project file within the same period of time as the decision to terminate the audit.

Defense Information Systems Agency Inspector General Comments

The DISA Inspector General agreed with the recommendation and stated that a checklist for terminated audits was added to the DISA OIG Audit Handbook in November 2020. The checklist includes a step to verify that documentation explaining the reason for the termination is included in the project file within the same period of time as the decision to terminate the audit. In addition, the DISA OIG audit staff was provided training on the checklist in November 2020.

[8] The DISA OIG audit organization conducted the Audit of Controls Over Contract Security Classification Specification (DD Form 254) (Project No. 16_IG21_001_400_AA) under the December 2011 GAS revision. The GAS 6.50 guidance is now contained in July 2018 revision to GAS, Section 5.25.

Our Response

Comments from the DISA Inspector General addressed all specifics of the recommendation. We verified that the checklist created for terminated audits includes a step to verify that documentation explaining the reason for the termination is included in the project file within the same period of time as the decision to terminate the audit. In addition, we verified that the DISA OIG audit staff was provided training on the checklist in November 2020. Therefore, the recommendation is closed.

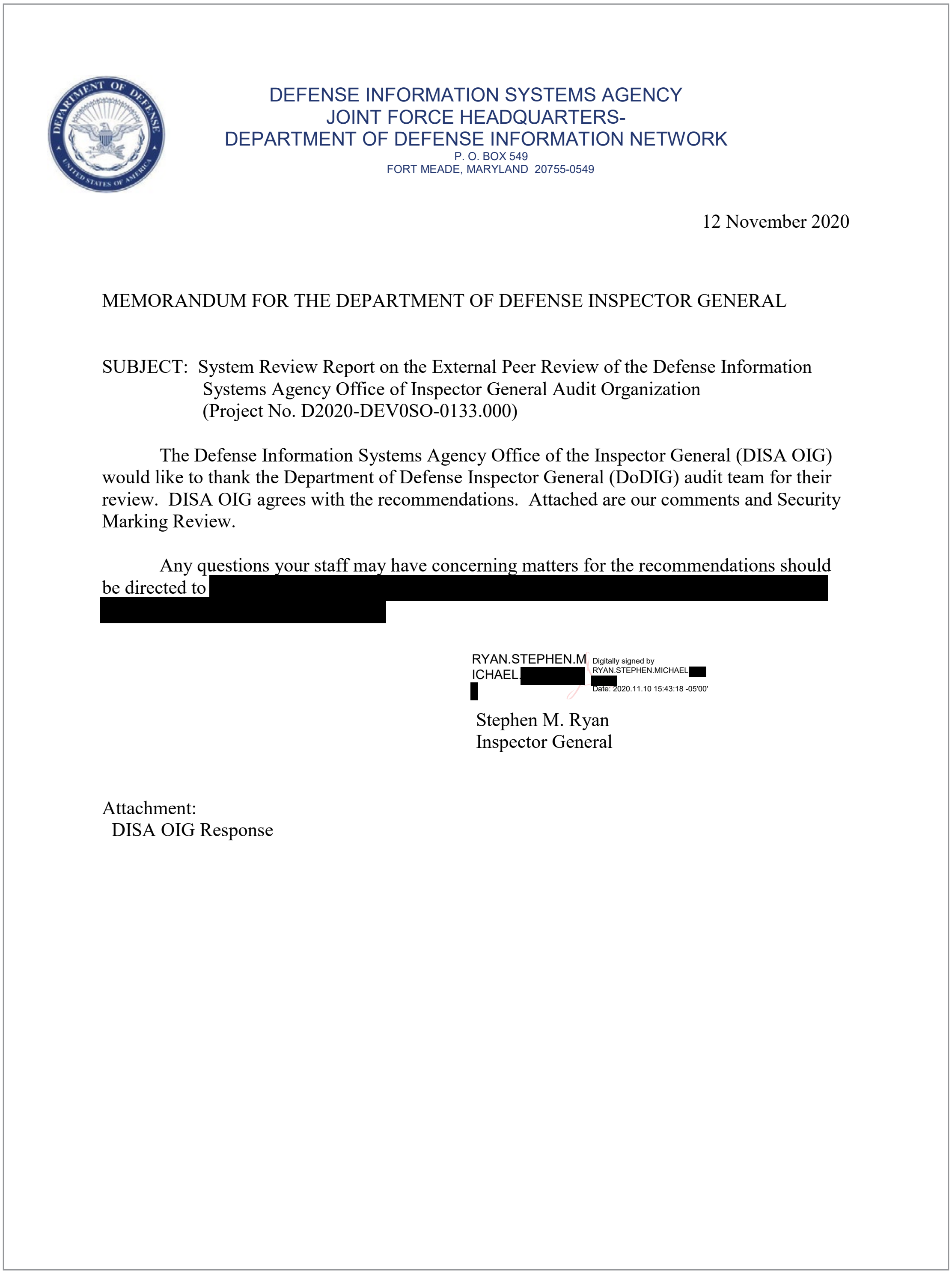
If you have any questions or would like to meet to discuss the report, please contact [redacted] We appreciate the cooperation and assistance we received during the peer review.

Randolph R. Stone
Assistant Inspector General for Evaluations
Space, Intelligence, Engineering, and Oversight

Enclosure 2

Management Comments

Defense Information Systems Agency Office of Inspector General (DISA OIG)



DEFENSE INFORMATION SYSTEMS AGENCY
JOINT FORCE HEADQUARTERS-
DEPARTMENT OF DEFENSE INFORMATION NETWORK
P. O. BOX 549
FORT MEADE, MARYLAND 20755-0549

12 November 2020

MEMORANDUM FOR THE DEPARTMENT OF DEFENSE INSPECTOR GENERAL

SUBJECT: System Review Report on the External Peer Review of the Defense Information Systems Agency Office of Inspector General Audit Organization (Project No. D2020-DEV0SO-0133.000)

The Defense Information Systems Agency Office of the Inspector General (DISA OIG) would like to thank the Department of Defense Inspector General (DoDIG) audit team for their review. DISA OIG agrees with the recommendations. Attached are our comments and Security Marking Review.

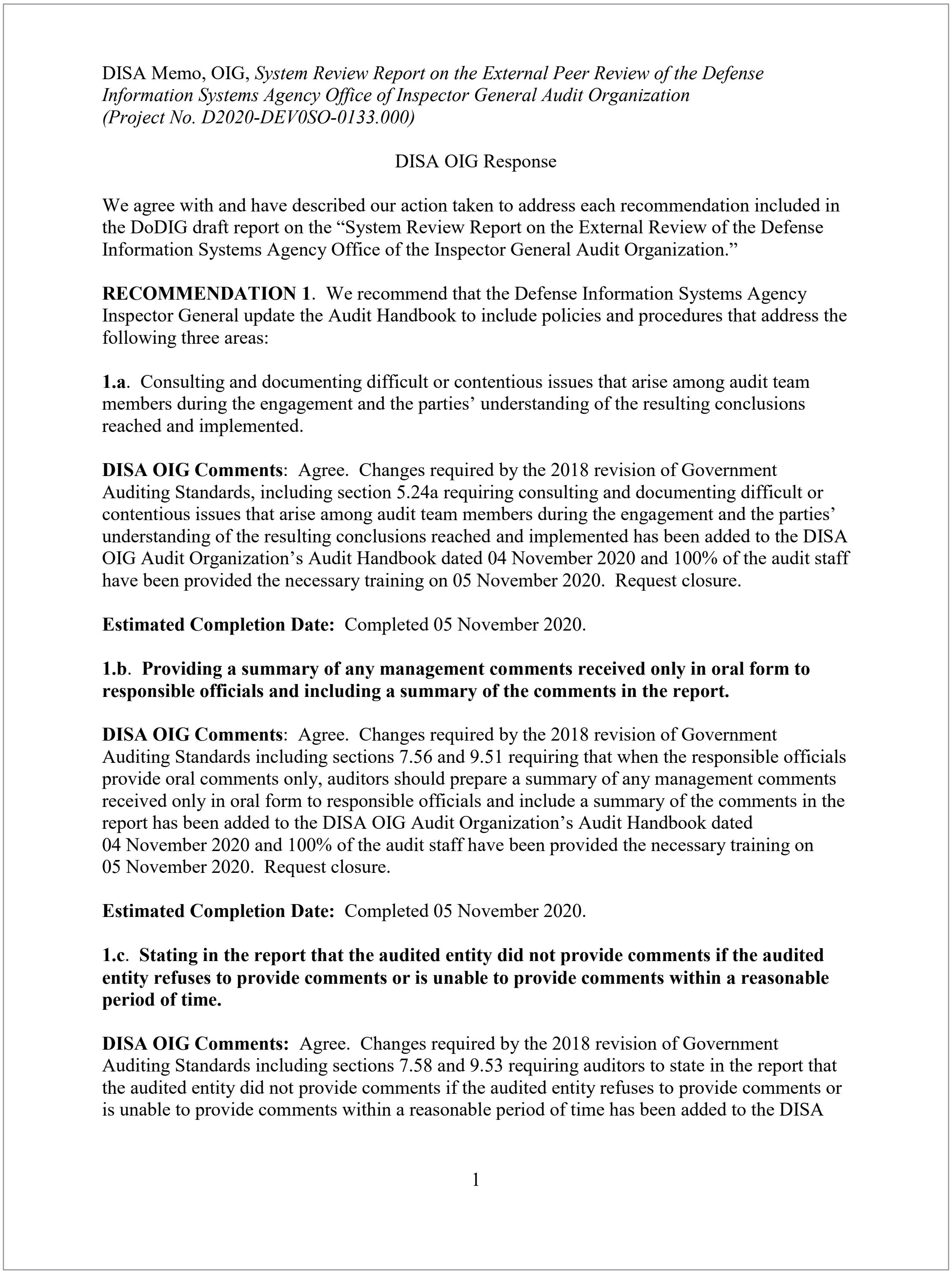
Any questions your staff may have concerning matters for the recommendations should be directed to [redacted]

RYAN.STEPHEN.M
ICHAEL [redacted]
Digitally signed by
RYAN.STEPHEN.MICHAEL [redacted]
Date: 2020.11.10 15:43:18 -05'00'

Stephen M. Ryan
Inspector General

Attachment:
DISA OIG Response

Defense Information Systems Agency Office of Inspector General (DISA OIG) (cont'd)



DISA Memo, OIG, *System Review Report on the External Peer Review of the Defense Information Systems Agency Office of Inspector General Audit Organization (Project No. D2020-DEV0SO-0133.000)*

DISA OIG Response

We agree with and have described our action taken to address each recommendation included in the DoDIG draft report on the "System Review Report on the External Review of the Defense Information Systems Agency Office of the Inspector General Audit Organization."

RECOMMENDATION 1. We recommend that the Defense Information Systems Agency Inspector General update the Audit Handbook to include policies and procedures that address the following three areas:

1.a. Consulting and documenting difficult or contentious issues that arise among audit team members during the engagement and the parties' understanding of the resulting conclusions reached and implemented.

DISA OIG Comments: Agree. Changes required by the 2018 revision of Government Auditing Standards, including section 5.24a requiring consulting and documenting difficult or contentious issues that arise among audit team members during the engagement and the parties' understanding of the resulting conclusions reached and implemented has been added to the DISA OIG Audit Organization's Audit Handbook dated 04 November 2020 and 100% of the audit staff have been provided the necessary training on 05 November 2020. Request closure.

Estimated Completion Date: Completed 05 November 2020.

1.b. **Providing a summary of any management comments received only in oral form to responsible officials and including a summary of the comments in the report.**

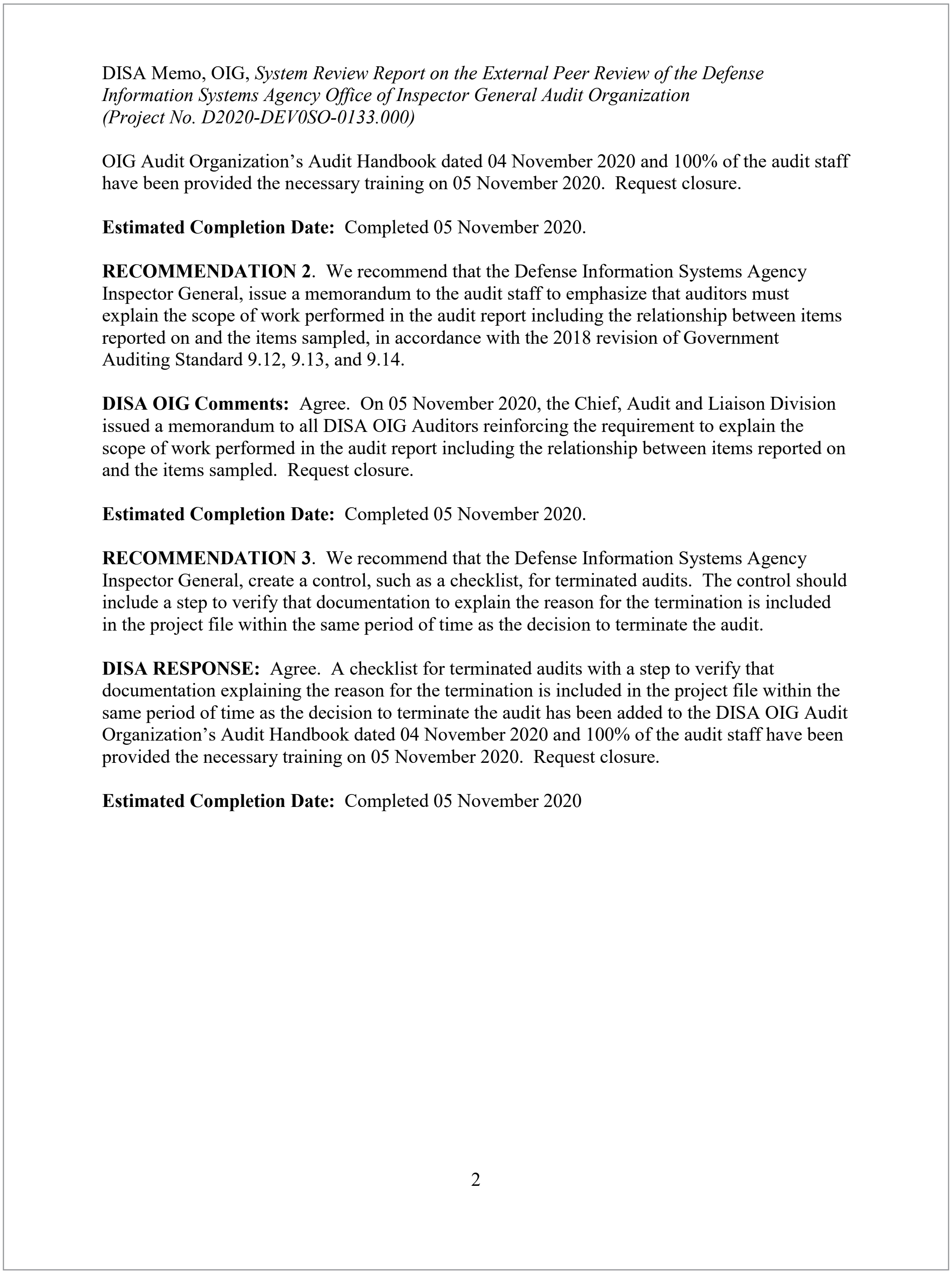
DISA OIG Comments: Agree. Changes required by the 2018 revision of Government Auditing Standards including sections 7.56 and 9.51 requiring that when the responsible officials provide oral comments only, auditors should prepare a summary of any management comments received only in oral form to responsible officials and include a summary of the comments in the report has been added to the DISA OIG Audit Organization's Audit Handbook dated 04 November 2020 and 100% of the audit staff have been provided the necessary training on 05 November 2020. Request closure.

Estimated Completion Date: Completed 05 November 2020.

1.c. **Stating in the report that the audited entity did not provide comments if the audited entity refuses to provide comments or is unable to provide comments within a reasonable period of time.**

DISA OIG Comments: Agree. Changes required by the 2018 revision of Government Auditing Standards including sections 7.58 and 9.53 requiring auditors to state in the report that the audited entity did not provide comments if the audited entity refuses to provide comments or is unable to provide comments within a reasonable period of time has been added to the DISA

Defense Information Systems Agency Office of Inspector General (DISA OIG) (cont’d)



OIG Audit Organization’s Audit Handbook dated 04 November 2020 and 100% of the audit staff have been provided the necessary training on 05 November 2020. Request closure.

Estimated Completion Date: Completed 05 November 2020.

RECOMMENDATION 2. We recommend that the Defense Information Systems Agency Inspector General, issue a memorandum to the audit staff to emphasize that auditors must explain the scope of work performed in the audit report including the relationship between items reported on and the items sampled, in accordance with the 2018 revision of Government Auditing Standard 9.12, 9.13, and 9.14.

DISA OIG Comments: Agree. On 05 November 2020, the Chief, Audit and Liaison Division issued a memorandum to all DISA OIG Auditors reinforcing the requirement to explain the scope of work performed in the audit report including the relationship between items reported on and the items sampled. Request closure.

Estimated Completion Date: Completed 05 November 2020.

RECOMMENDATION 3. We recommend that the Defense Information Systems Agency Inspector General, create a control, such as a checklist, for terminated audits. The control should include a step to verify that documentation to explain the reason for the termination is included in the project file within the same period of time as the decision to terminate the audit.

DISA RESPONSE: Agree. A checklist for terminated audits with a step to verify that documentation explaining the reason for the termination is included in the project file within the same period of time as the decision to terminate the audit has been added to the DISA OIG Audit Organization’s Audit Handbook dated 04 November 2020 and 100% of the audit staff have been provided the necessary training on 05 November 2020. Request closure.

Estimated Completion Date: Completed 05 November 2020

Acronyms and Abbreviations

CIGIE	Council of the Inspectors General on Integrity and Efficiency
DFARS	Defense Federal Acquisition Regulation Supplement
DISA	Defense Information Systems Agency
GAS	Government Auditing Standard
GSA	General Services Administration
IT	Information Technology

INSPECTOR GENERAL

INTEGRITY EFFICIENCY

DEPARTMENT OF DEFENSE

Whistleblower Protection

U.S. Department of Defense

Whistleblower Protection safeguards DoD employees against retaliation for protected disclosures that expose possible waste, fraud, and abuse in government programs. For more information, please visit the Whistleblower webpage at http://www.dodig.mil/Components/Administrative-Investigations/Whistleblower-Reprisal-Investigations/Whisteblower-Reprisal/ or contact the Whistleblower Protection Coordinator at Whistleblowerprotectioncoordinator@dodig.mil

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

Congressional Liaison
703.604.8324

Media Contact
public.affairs@dodig.mil; 703.604.8324

DoD OIG Mailing Lists
www.dodig.mil/Mailing-Lists/

Twitter
www.twitter.com/DoD_IG

DoD Hotline
www.dodig.mil/hotline

DEPARTMENT OF DEFENSE | INSPECTOR GENERAL

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