STATEMENT OF WORK FOR FISCAL YEAR 2004 AUDIT OF THE DEFENSE INFORMATION SYSTEMS AGENCY COMPUTER SERVICES
RFQ 35438

1.0 INTRODUCTION

The Office of the Inspector General of the Department of Defense, (IG DoD), Defense Financial Auditing Service (DFS) requires an information assurance and compliance audit of the Defense Information Systems Agency (DISA) Computer Services.

2.0 OBJECTIVE

The contractor shall perform the audit of DISA in accordance with Generally Accepted Government Auditing Standards (GAGAS). The contractor shall use the General Accounting Office (GAO) Federal Information Systems Controls Audit Manual (FISCAM) and Statements on Auditing Standards (SAS) 70/88 to develop the methodology and detailed audit steps to determine DISA compliance with Business Management Modernization Program Systems Compliance Criteria, DoD information assurance policy including the DoD Information Technology Security Certification and Accreditation Process (DITSCAP), the Federal Financial Management Improvement Act (FFMIA) of 1996, and DISA Security Technical Implementation Guides (STIGs), and the Federal Information Security Management Act (FISMA). The purpose of this audit will determine whether DISA is secure and compliant with applicable guidance to produce accurate and reliable data. Specifically, the contractor will determine whether DISA: (1) general and application controls are adequately designed and effective; (2) complies with the FFMIA and all other applicable laws and regulations; and (3) is properly certified and accredited in accordance with DITSCAP.

3.0 BACKGROUND

The IG DoD is implementing a long-range strategy to conduct audits of DoD financial statements. The Chief Financial Officer's Act of 1990 (P.L. 101-576), as amended by the Government Management Reform Act of 1994, mandates that agencies prepare financial statements and conduct audits of the financial statements. To meet that requirement, the IG DoD will audit information systems that provide supporting data to financial statements.

DISA provides computing services that enable the DoD community to execute its mission. The computing services encompass mainframe, server, and other information processing across a broad spectrum of operating system. DISA is the DoD's number one provider of personnel, payroll, logistics, accounting, and medical records processing. The DISA computing environment has approximately 800,000 users and process 1,400 applications at 18 data centers.

Each DISA Defense Enterprise Computing Center (DECC) has one to five Detachments that provide technical expertise for the environments in which they operate.

General Controls. General controls are the policies and procedures that apply to all or a large segment of the entity's information systems and help ensure proper operation. Examples of primary objectives for general controls are to safeguard data, protect computer

application programs, prevent system software from unauthorized access, and ensure continued computer operation in case of unexpected interruptions. The FISCAM describes six major categories of general controls; access controls, application software development and change controls, system software controls, segregation of duties, entity wide security program planning and management, and service continuity.

Application Controls. Application controls are directly related to individual computerized applications owned and operated by DISA to manage, operate, and secure the computing environment. They help ensure that transactions are valid, properly authorized, and completely and accurately processed and reported. Application controls include (1) programmed control techniques, such as automated edits; and (2) manual follow-up of computer-generated reports, such as reviews of reports identifying rejected or unusual items.

Both general and application controls must be effective to help ensure the reliability, appropriate confidentiality, and availability of critical automated information.

3.1. LOCATIONS. DISA has five DECCs located in Columbus, OH; Oklahoma City, OK; St Louis, MO; Mechanicsburg, PA; and Ogden, UT. The DECCs and Detachments are:

Defense Enterprise Computing Center, Mechanicsburg, PA
DECC Detachment Chambersburg, PA
DECC Detachment San Diego, CA
DECC Detachment Norfolk, VA
DECC Detachment Puget Sound, WA

Defense Enterprise computing Center Oklahoma City, OK
DECC Detachment Montgomery, AL
DECC Detachment Warner Robins, GA
DECC Detachment San Antonio, TX

Defense Enterprise Computer Center, St Louis, MO
DECC Detachment Huntsville, AL
DECC Detachment Rock Island, IL

Defense Enterprise Computing Center, Columbus, OH
DECC Detachment Denver, CO
DECC Detachment Indianapolis, IN

Defense Enterprise Computing Center, Ogden UT
DECC Detachment Dayton, OH

3.2. PRIOR AUDITS. The IG DoD, GAO, and the Service audit agencies have conducted numerous audits of Defense Information Systems Agency Computer Services. These audit reports can be found on entity web sites.

3.3. CONTRACTING OFFICER REPRESENTATIVE (COR). The IG DoD will appoint a Contracting Officer Representative (COR) at the task order level. The COR will oversee the audit in accordance with Financial Audit Manual (FAM) 650 and will approve all deliverables.

3.4. FINANCIAL STATEMENTS AND LINE ITEMS SUPPORTED BY DISA COMPUTING SERVICES. The DISA Computing Services indirectly supports the financial statements and line items by providing file extractions to multiple agencies to be included in their financial statements.

4.0 GUIDANCE/APPLICABLE DOCUMENTS:

The contractor shall use the GAO FISCAM and SAS 70/88 to develop the methodology and detailed audit steps to determine DISA compliance with Business Management Modernization Program Systems Compliance Criteria, DoD information assurance policy including DITSCAP, FFMIA, STIGs, and FISMA. The following documents are applicable to this task order.

4.1. Public Law 107-347, "E-Government Act," December 17, 2002, includes Title III, the Federal Information Security Management Act (FISMA). The FISMA permanently reauthorized the framework laid out in the Government Information Security Reform Act. FISMA requires protection of all information and information systems, including those owned or operated outside the agency. Agency information technology security programs apply to all organizations (sources) that possess or use Federal information. The FISMA provides (1) effective government-wide management and oversight of the related information security risks, including coordination of information security efforts throughout the civilian, national security, and law enforcement communities; (2) development and maintenance of minimum controls required to protect Federal information and information systems; and (3) a mechanism for improved oversight of Federal agency information security programs. In addition, it acknowledges that commercially developed information security products offer advanced, dynamic, robust, and effective information security solutions, reflecting market solutions for the protection of critical information infrastructures important to the national defense and economic security of the nation that are designed, built, and operated by the private sector. Lastly, FISMA recognizes that individual agencies should select specific technical hardware and software information security solutions from among commercially developed products.

4.2. Public Law 101-576, the "Chief Financial Officer's Act of 1990," as amended by the Government Management Reform Act of 1994, requires the DoD to prepare annual financial statements for audit. As a result, controls must be evaluated to assess the accuracy and completeness of computer-processed data supporting the financial statements.

4.3. Public Law 104-208, the "Federal Financial Management Improvement Act of 1996" requires each agency to implement and maintain financial management systems that comply substantially with:

- Federal financial management system requirements;
- applicable Federal accounting standards; and
- the United States Government Standard General Ledger at the transaction level.

4.4. GAO-03-673G, "Government Auditing Standards," June 2003, issued by the GAO contains the standards for audits of government organizations, programs, activities and functions, and of government assistance received by contractors, nonprofit organizations, and other non-government organizations. Auditors and audit organizations when required by law, regulations, agreement, contract, or policy must follow these standards, often referred to as Generally Accepted Government Auditing Standards (GAGAS). These standards pertain to auditors' professional qualifications, the quality of audit effort, and the characteristics of professional and meaningful audit reports.

4.5. The GAO/President's Council on Integrity and Efficiency Financial Audit Manual, July 2001, provides the requirements for performing financial statement audits of Federal entities.

4.6. SAS 70, "Service Organizations," as amended by SAS 88, is a standard developed by the American Institute of Certified Public Accountants (AICPA) and is the authoritative guidance that allows service organizations to disclose their control activities and processes to customers and customer auditors in a uniform reporting format. SAS 88 adds guidance on service organization information systems. A SAS 70/88 audit or examination represents that a service organization has performed an in-depth audit of its control activities including controls over information technology and related processes.

4.7. The GAO Federal Information Systems Controls Audit Manual (FISCAM) January 1999 or latest version (GAO/AIMD-12.19.6, Volume 1), describes the computer-related controls that auditors should consider when assessing the integrity, confidentiality, and availability of computerized data. This manual is primarily designed for evaluations of general and application controls over financial information systems that support agency business operations. Its purposes are to (1) inform financial auditors about computer-related controls and related audit issues so that they can better plan their work and integrate the work of information systems (IS) auditors with other aspects of the financial audit and, (2) provide guidance to IS auditors on the scope of issues that generally should be considered in any review of computer-related controls over the integrity, confidentiality, and availability of computerized data associated with federal agency systems.

4.8. National Institute of Standards & Technology (NIST) Standards. The NIST standards provide government-wide methods and procedures to assess the security controls in Federal information systems. If needed, an agency may supplement these methods and procedures.

4.9. DoD Directive 8500.1, "Information Assurance," October 24, 2002, establishes guidelines under Section 2224 of title 10, United States Code, "Defense Information Assurance Program," to achieve DoD information assurance through a defense-in-depth approach that integrates the capabilities of personnel, operations, and technology, and supports the

evolution to network centric environments. Additionally, this directive requires all DoD information systems to maintain an appropriate level of confidentiality, integrity, authentication, non-repudiation, and availability that reflect a balance between the importance and sensitivity of the information and information assets.

4.10. DoD Directive O-8530.1, "Computer Network Defense (CND)," January 8, 2001, (FOUO) mandates all owners of DoD information systems and computer networks to enter into a service relationship with a CND provider.

4.11. DoD Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation Process," December 30, 1997, implements DoD Directive 5200.40 by establishing a standard DoD-wide process, set of activities, general tasks, and a management structure to certify and accredit information systems that will maintain the information assurance and security posture of the Defense information infrastructure, throughout the life cycle of the system. In addition, DoD Manual 8510.1, "DoD Information Technology Security Certification and Accreditation Process Application Manual," July 31, 2000, provides implementing guidance to standardize the Defense Information Technology Security Certification and Accreditation Process throughout the DoD.

4.12. DoD Instruction 8500.2, "Information Assurance Implementation," February 6, 2003, implements policy, assigns responsibilities and prescribes procedures for applying integrated layered protection of the DoD information systems and networks under DoD Directive 8500.1, "Information Assurance," October 24, 2002. Additionally, it authorizes the publication of DoD 8500.2-H, consistent with DoD 5025.1-M, "DoD Directives Systems Procedures," current edition.

4.13. DoD 8510.1-M, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP) Application Manual," July 31, 2000, issued under the authority of DoD Instruction 5200.40 is mandatory for use by all DoD components. It provides implementation guidance to standardize the information system and network certification and accreditation process throughout DoD.

4.14. Security Technology Implementation Guides. DoD Directive 8500.1 establishes policy and assigns DISA responsibility to develop and provide security configuration guidance for information assurance (IA) and IA-enabled products. The DISA Field Security Operations (FSO), in coordination with the National Security Agency, develops STIGs to provide standardized approved security configuration guidelines that are applicable to all IA and IA-enabled information technology products incorporated into DoD information systems. The FSO conducts independent Security Readiness Reviews of DISA to evaluate systems compliance with the STIGs.

5.0 AUDITS OF DOD FINANCIAL MANAGEMENT SYSTEMS

5.1. METHODOLOGY. The contractor shall perform an audit of DISA Computing Services (all DECCs including Detachments)using FISCAM and SAS 70/88 guidance. The contractor will determine whether general and application controls are effective in design and operation and may be relied on to support CFO audit work. Additionally, the contractor shall also assess whether DISA Computing Services complies with FFMIA requirement and all other applicable laws and regulations, and is properly certified and accredited in accordance with DITSCAP. certification and accreditation requirements, and other applicable laws and regulations.
Consistent with the FAM, the audit will consist of planning and internal controls, testing, and reporting phases. Throughout each phase, the contractor shall immediately report insufficient controls and recommend corrective actions at that time. The contractor shall conduct the audit project in compliance with financial audit methodology set forth in current versions of the FAM and FISCAM.

5.2. DELIVERABLES. This task order includes the following deliverables for planning and internal controls, testing, and reporting phases. Attachment 1 provides a list of deliverables and the number of days after contract award that the deliverables are due. The contractor shall deliver all audit products in Microsoft Office compatible electronic format, as well as any hard copy documents not included in the electronic files.

5.2.1 PHASE I - PLANNING AND INTERNAL CONTROLS. The planning and internal controls phase of this task order applies only to developing the audit plan including a network diagram and test plan; oral presentations; providing a travel plan; and submitting deliverables that are in conformity with guidance in Section 4.0,"Guidance/Applicable Documents". During the planning and internal controls phase, the contractor shall complete the following:

- gain an understanding of DISA operations and identify controls and operations that are significant to the audit,
- assess inherent risk and control risk,
- make a preliminary assessment on whether general controls are likely to be effective, and
- identify the controls that will be tested.

The following deliverables must be completed during the planning and internal control phase.

5.2.1.1 KICKOFF AND ENTRANCE CONFERENCE. The contractor shall hold a kick off conference with the IG DoD prior to the entrance conference. The contractor shall then hold a formal entrance conference with key agency officials and the COR. The entrance conference will include a discussion of contractual requirements. The date of the entrance conference will be determined in conjunction with the COR.

5.2.1.2 IN PROCESS REVIEW. The contractor shall also be required to provide 2 in-process reviews (IPR) to the DISA and their auditor. The first IPR will be at completion of the planning phase to give the user organizations an opportunity to provide input on the internal controls that need to be addressed in the SAS 70/88 report. The date for the second IPR will be determined by the COR in conjunction with the contractor.

5.2.1.3 AUDIT PLAN. The contractor shall develop an audit plan to evaluate DISA information system integrity, availability, confidentiality, authentication, and non repudiation in accordance with DoD Financial Management Regulations (DoD FMR); and DoD Instruction 8500.2, "Information Assurance Implementation." The audit plan must include a risk assessment of DISA in accordance with DITSCAP. The contractor must base the audit plan on FISCAM and FAM augmented with DoD Instruction 8500.2 for information assurance controls and DoD 8510.1-M for testing. If needed, the contractor shall develop additional audit steps to ensure compliance with applicable laws and regulations, and identify those steps in the audit plan. Additionally, the contractor shall include steps in the audit plan to evaluate and to the extent possible rely on completed DITSCAP and STIG testing to avoid unnecessary duplicative efforts.

The audit plan must include the audit approach, scope, methodology, nature and type of testing, qualitative measurement standards, and reporting requirements that best achieves the audit objectives in a cost effective and timely manner. Further, the audit plan must include steps to assess system attributes and a matrix of metrics used to determine compliance. These attributes must comply with the DoD standards listed in Section 4.0, "Guidance/Applicable Documents."

5.2.1.3 UNDERSTANDING DISA. The contractor shall first develop and document a high-level understanding of DISA in accordance with the FISCAM, Section 2.1.

5.2.1.4 ASSESS INHERENT RISK AND CONTROL RISK. After gaining an understanding of the entity's operations, the contractor shall assess the inherent and control risks that are considered when determining audit risk.

The contractor shall (1) identify conditions that significantly increase inherent and control risks and (2) conclude whether they preclude the effectiveness of specific control techniques in significant applications. The contractor identifies specific inherent risk and control structure weaknesses based on information obtained in the planning and internal controls phase, primarily from understanding DISA operations.

For each inherent risk or control structure weakness identified, the contractor shall document the nature and extent of the risk or weakness, the conditions (s) that gave rise to that risk or weakness; and the specific information or operations affected (if not pervasive). The contractor shall also document other consideration that may mitigate the effects of identified risks and weaknesses.

5.2.1.5 PRELIMINARY ASSESSMENT OF CONTROLS. As part of assessing control risk, the contractor shall make a preliminary assessment on whether computer-related controls are likely to be effective. This assessment is based preliminary on discussions with personnel throughout the entity, including program managers, system administrators, information resource managers, and systems security managers; on observations of computer-related operations; and on cursory reviews of written policies and procedures.

The contractor should use the summary tables in Appendix III, FISCAM, which are also available in electronic form from GAO's World Wide Web server, to document preliminary findings and to assist in making the preliminary assessment of controls. (GAO's Internet address is: http://www.gao.gov)

5.2.1.6 IDENTIFY CONTROLS TO BE TESTED. Based on assessments of inherent and control risks, including the preliminary evaluation of computer-based controls, the contractor shall identify the general control techniques that appear most likely to be effective and should therefore be tested to determine if they are in fact operating effectively. By relying on these preliminary assessments to plan audit tests, the contractor can avoid expending resources on testing controls that clearly are not effective. The tables in Appendix IV, FISCAM, are provided for use in concluding the control effectiveness and for summarizing an overall assessment for each control category. These tables are also available in electronic form from GAO's World Wide Web server. As required by GAO/OCG-94-4, "Government Auditing Standards" (commonly known as "the Yellow Book"), which sets forth GAGAS, the contractor must, when possible and with the approval of the COR, rely on the work of others that falls within the scope and objectives of this task order. The test plan must include sufficient procedures to provide a basis for reliance on the work of others. For those systems that have met the requirements for DITSCAP certification and accreditation, the contractor shall review test documentation, and if necessary, observe system demonstrations. If information assurance tests are required, then the contractor should base test procedures on the system certification level as defined in DITSCAP. The contractor must obtain a waiver from the system owner prior to any penetration testing.

Level 2 > Security Test and Evaluation (ST&E)	ST&E validates known security features of the system
Level 3 and up > ST&E and Penetration Testing	Penetration Tests are penetration attempts both inside and outside on known vulnerabilities.

Security test plans must evaluate the effectiveness of system and network interface security features. In addition, the test plan must include a review of application controls that ensure data accuracy and reliability, such as procedures to test data entry, data processing, and protection from unauthorized modifications or damage.

In developing the internal controls segment of the test plan, the contractor must identify all relevant significant laws, policies, regulations, and guidelines and include compliance testing procedures. The plan must be documented, approved by the COR, and kept current.

The contractor shall provide draft and final audit and test plans for COR review and approval. The contractor will not begin work on Phase 2 until the COR has reviewed and approved the plans.

5.2.2 PHASE II - TESTING. In accordance with FISCAM and DITSCAP, the contractor must perform an assessment of DISA computing services to determine whether general and application controls are properly designed and operating effectively, complies with FFMIA requirements and all other applicable laws and regulations, and is properly certified and accredited in accordance with DITSCAP. The contractor must conduct all tests in accordance with approved test plans and should take into account DITSCAP and system security reviews already completed.

In evaluating and testing the DISA information system internal controls, the contractor must determine DISA compliance with all significant laws, policies, regulations, and guidelines in accordance with compliance procedures in the test plan.

The evaluation and testing will include all applicable mandatory baseline controls found in DoDI 8500.2 and AR 25-2 documented in the specific control evaluations (or similar documents) prepared during the planning and internal control phase. For those controls that the contractor deems to be ineffectively designed or not operating as intended, the contractor shall gather sufficient evidence to support appropriate findings and to provide recommendations to improve controls. The following deliverables will be completed during the testing phase:

5.2.2.1 EXIT CONFERENCE. The contractor shall hold a formal exit conference with key agency officials and the COR. The contractor will determine the date of the exit conference in conjunction with the COR.

5.2.3 PHASE III REPORTING. The contractor shall complete following deliverables during the reporting phase.

5.2.3.1 DRAFT REPORT: The contractor shall provide to the IG DoD a draft report package no later than 30 days after the end of audit fieldwork. The draft report package will include a cross-referenced SAS 70/88 Type II report, a technical report for each DECC, updated network diagram, and a management letter. The draft report must address the audit objectives in Section 2.0. The COR will review and approve the draft report package.

5.2.3.2 FINAL REPORTS. The contractor will provide the IG DoD with a final audit report package no later than 10 working days after receipt of IG DoD final comments on the draft report package. The final report package will contain a cross-referenced SAS 70/88 Type II report and a technical report. The COR will review and approve the final report package.

5.2.3.3 TECHNICAL REPORT. The contractor shall provide a technical report within 30 days of completing the review of each DECC and the applicable Detachments. The report must document the control tests performed including test results; and conclusions and recommendations (or proposed corrective actions) related to each procedure performed using the condition, cause, methodology, criteria, and effect structure. The contractor must clearly develop each reportable condition and material weakness. The report will include an introduction, background, scope, methodology, overall summary of results, and a description of the system environment. The report will document the tests of controls, data flows, and compliance with applicable laws and regulations. The report must conclude whether certification and accreditation complies with DITSCAP. The COR will review and approve the technical report.

5.2.3.3 TYPE II REPORT. The contractor must prepare a SAS 70/88 Type II Report for DISA Computing Services, as a whole.

5.2.3.4 MANAGEMENT LETTER. The contractor must prepare a management letter. The management letter will consist of two parts, one of which will contain only information that is sensitive in nature. The management letter will include findings, conditions, or concerns that the contractor identified but that are not significant enough to warrant being included in the audit report. The contractor must address the management letter to the IG DoD with copies to management. The COR will review and approve management letters prior to issuance.

6.0 REQUIREMENTS/ADMINISTRATION

6.1 AUDIT DOCUMENTATION. The contractor shall prepare audit documentation in accordance with GAGAS. The contractor shall provide the IG DoD access to audit documentation throughout the duration of the contract to ensure compliance with applicable Government Auditing Standards. Audit documentation includes but is not limited to: planning documentation; audit program guides; working paper documentation; summaries; flowcharts and related documentation; risk assessment matrices; results and documentation of detailed testing procedures; support for the conclusions made as a result of detailed testing; support for findings; and evidence of supervision. The audit documentation must contain sufficient information to enable an experienced auditor who has had no previous connection with the audit to ascertain from the audit documentation the evidence that supports the auditors' significant judgments and conclusions. The contractor with prior approval from the IG DoD must also make audit documentation available to GAO at no additional cost.

Audit documentation must describe audit procedures and be cross-referenced to audit programs, related audit documentation, and the audit report. The audit documentation must fully support audit findings and conclusions. The audit documentation should include a description of the purpose, source, scope, methodology, criteria, conclusions, and recommendations related to the work performed. The audit plan must document audit steps, testing and sampling procedures, and the methodology. In addition, audit

documentation must adequately address the internal controls and include a substantive testing plan, risk assessment, and related specific control evaluations. Audit documentation must fully describe the nature and extent of information used to identify internal control weaknesses and reportable conditions. The contractor shall summarize other potential reportable conditions separately. The contractor must mark all audit documentation and supporting documents as property of the IG DoD.

The contractor shall deliver to the IG DoD any application software, to include upgrades and patches necessary to access audit documentation at no additional cost to the IG DoD. The contractor shall grant a limited license to the IG DoD to use the provided application software to access delivered audit documentation throughout the IG DoD retention of the audit documentation. If requested, the contractor shall provide up to 8 hours of training to both IG DoD and GAO staff on the use of any application software to access and review delivered working papers. All audit documentation is the property of the IG DoD and will be retained by IG DoD. The contractor must deliver all audit documentation to the IG DoD with the draft audit report package. Audit documentation revised subsequent to the delivery of audit documentation contained in the draft audit report package must be delivered to the IG DoD with the final audit report package. Contractors may retain copies of audit documentation for their files.

6.2 SECURITY. The contractor is responsible for obtaining employee security clearances, where required, and for providing proof of such clearances to each site visited. The contractor must also ensure that all persons working on this effort are US citizens. The contractor must promptly initiate the clearance process with Defense Industrial Security, through the contractor's security staff. See Attachment 2, "Department of Defense Contractor Security Classification Specification" (DD Form 254), for security requirements and information. For access to facilities, a National Agency Check with Local Agency and Credit Check (NACLC) is generally sufficient. The Defense Information Systems Agency requires an ADP-1 Critical-Sensitive classification in accordance with DoD 5200-R, "Personnel Security Program," Change 3, dated February 23, 1996, for access to systems.

The contractor must handle all documents relating to this task order using "For Official Use Only" security procedures. Review DoD Regulation 5200.1-R for proper handling of "For Official Use Only" material.

6.3 STAFFING.

6.3.1 **KEY PRESONNEL.** The contractor will provide the Procuring Contracting Officer (PCO) with a list of the key personnel at the senior level and above assigned to the contract. After contract award, the contractor may not substitute names without prior written approval from the PCO. The contractor will not be paid for key personnel billed to the task order without prior written authority from the PCO.

6.3.2 ASSIGNED STAFF. The contractor must submit a list of assigned staff and their qualifications to the COR with the audit plan. The staff listing must also include the security clearance of each individual. The COR shall approve all audit staff revisions.

6.3.2 SUB-CONTRACTOR INFORMATION. Prior to contract award, the prime contractor must provide the names, addresses, and qualifications of all anticipated subcontractors that will perform work on the task order. In addition, the sub-contractors must meet the independence requirements in Section 6.8.

6.4 HOURS. The contractor shall not perform work on weekends or holidays without prior approval of the COR. The only exception is for the observance of the following holidays: Independence Day, Labor Day, Columbus Day, Veterans Day, and Martin Luther King Jr.'s Birthday. The contractor will not work over 10 hours per day and more than 50 hours per week without prior approval of the COR. The COR has no authority to change this element of the task order without further negotiation. Work outside the scope of this SOW should be documented on a lead sheet and presented to the COR for consideration of a follow-on task order.

6.5 TRAVEL PLAN. The contractor must provide travel plans in writing to the COR no less than 10 workdays prior to travel.

6.6 OTHER DIRECT COSTS. The contractor must provide other direct costs in writing to COR, with support documentation/justification, prior to incurring cost.

6.7 CONFIDENTIALITY. The contractor shall hold all material and information gained from the IG DoD or other DoD activities in connection with this task order in strict confidence and not make use thereof, other than for the performance of this task order. The contractor shall release such material and information only to its employees requiring such information in the "need-to-know" discharge of their duties under this task order and to the IG DoD, and not release or disclose the same to any other party, unless directed to do so by the Contracting Officer. Those employees with a "need-to-know" discharge must sign a Non-Disclosure Agreement.

6.8 INDEPENDENCE. The contractor in a separate statement must represent that it is independent, as defined in Government Auditing Standard 3.03 and 3.04 with respect to DISA. In this separate statement, the contractor must briefly describe all work and known future work, including non-audit services, related to DISA in the past 5 years. In addition, throughout the performance of the task order, the contractor must also immediately inform the COR in writing if the contractor is considering to propose or has already proposed on any contracts directly or indirectly involving DISA. The notification to the COR must include the type of contract services to be performed and the period covered. The COR will then evaluate whether award of these contracts could impair the contractor's independence.

6.9 PROGRESS REPORTING. The contractor shall provide progress reports to the COR at least bi-weekly throughout the term of the task order. The progress reports shall communicate the contractor's progress/performance, identification of performance problems, recommended corrective actions and other pertinent issues. At the COR's discretion, progress briefings can be provided using video teleconferencing, telephone, e-mail, or in person.

6.10 IMMEDIATE NOTIFICATION. In addition to the progress reports the contractor shall discuss with the COR and management any matter that comes to the auditor's attention that would significantly affect their opinion on DISA Computing Services or that significantly affect the report or outcome of other services that may be provided. During the course of all services provided under this contract, the contractor must immediately notify the COR of any issues identified which may pose a significant operation or financial management problem or indicate the possibility of fraud or abuse.

6.11 OTHER COMMUNICATION. In accordance with the AICPA's "Statement on Auditing Standards," section 315.11 0-Other Communications, a successor contractor may wish to obtain access to the predecessor's audit documentation. In these circumstances, the contractor should request the IG DoD to authorize such access.

6.12 ASSISTANCE TO CONTRACTOR. In addition to the duties described elsewhere in this task order, IG DoD personnel will be available to attend meetings and to provide assistance in obtaining requested data or access.

6.13 EVALUATION OF PROPOSALS. Each bidder must submit a Statement of Independence and a list of prior clients we can contact to discuss the quality of bidder's prior work. Bids submitted without a Statement of Independence and/or a list of prior clients will not be evaluated.

6.14 METRICS. This task order will be performance based. As such, the following metrics are required.

6.14.1 PERFORMANCE METRIC. The purpose of the requirements and standards in section 4.0 is to provide a methodology for performing the audit and ensure that the audit achieves its intended outcome. The COR will measure the contractor's performance against the standards and other guidance associated with performing this audit.

6.14.2 SCHEDULE METRIC. The actual accomplishment of the schedule will be assessed against the original due dates and milestones established for this task order.

6.14.3 COST METRIC. The COR will determine the variance between the contractor's proposed cost and the actual costs. The COR will analyze and determine the reason for any variance.