STATEMENT OF WORK FOR AUDIT OF THE
DEFENSE PROPERTY ACCOUNTABILITY SYSTEM

1.0 INTRODUCTION

The Office of the Inspector General of the Department of Defense (IG DoD), Defense Financial Auditing Service (DFS) requires audit services to conduct information assurance and compliance audit on the Defense Property Accountability System (DPAS).

2.0 OBJECTIVE

The contractor shall perform the audit of DPAS controls 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) to develop the methodology and detailed audit steps to determine DPAS compliance with Business Management Modernization Program Systems Compliance Criteria, the DoD Information Technology Security Certification and Accreditation Process (DITSCAP), and Statement on Auditing Standards (SAS) 70/88. The purpose of this audit project will be to determine whether DPAS is secure and compliant with applicable guidance to produce accurate and reliable data. Specifically, the contractor will determine whether DPAS: (1) general and application controls are adequately designed and effectively operating; (2) complies with all relevant Federal Financial Management Improvement Act (FFMIA) requirements and 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 financial statements. To meet that requirement, the IG DoD will audit controls of information systems that provide supporting data to financial statements.

DPAS is a standard property system with on-line capability to support all functions that are associated with property accountability and asset management. DPAS will allow the DoD to accurately collect financial property information, update the general ledgers, impose financial control over real and personal property, and depreciate capital assets. DPAS interfaces with other accounting and logistics systems to receive and/or provide data for more integrated property management and improved financial reporting.

General Controls. General controls help to ensure the proper operation of the financial management system. The primary purpose of the general controls are to safeguard data, protect computer application programs, prevent unauthorized access, and ensure continued computer operation in case of unexpected interruptions. The General Accounting Office (GAO) 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 the structure, policies, and procedures that apply to separate, individual application systems, such as accounts payable, inventory, payroll, grants, or loans. An application system is typically a collection or group of individual computer programs that relate to a common function. In the Federal government, some applications may be complex, comprehensive systems, involving numerous computer programs and organizational units, such as those associated with benefit payment systems. Application controls encompass both the routines contained within the computer program code, and the policies and procedures associated with user activities, such as manual measures performed by the user to determine that data were processed accurately by the computer.

3.1. LOCATIONS. The developmental version of DPAS is supported by Defense Enterprise Computing Center – Detachment, Dayton (DECC-D), Wright Patterson Air Force Base, Dayton, Ohio. The developers have remote access through their LAN. The Defense Information Systems Network provides the required telecommunications support to assure connectivity between the component installations and the servicing DECC-D. Production services are provided by DECC-D, Dayton, Ohio.

DPAS runs on HP 9000 K-series, L2000 series, and RP5450 series model servers. It uses the HP-UX 11.X Operating System. DPAS supports multiple relational databases and the database management system software utilized is the SUPRA NT product Supra Server SQL, Release 29.00.00 (SUPRANT29.00.00). The application server software is written in Micro Focus ANSI 85 COBOL with embedded SQL and UNIX Shell Scripts. Other server software used is Micro Focus AAI and IQ Smart Server. Client software DPAS executables include Eureka and SUPRA Server SQL.

3.2. PRIOR AUDITS. There have been a number of audit reports issued related to this task order. The COR will provide the list of prior audits on request.

Report No. 98-135, “Implementation of the Defense Property Accountability System,” May 18, 1998, in which we reviewed the capabilities of Defense Property Accountability System (DPAS) to provide custodial and financial accountability for personal and real property.

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. SYSTEM INTERFACES. Unit Level Logistics System S-4 (ULLS-S4); Army Master Data File (AMDF); Supply Bulletin 700-20 (SB 700-20); Army's National Defense Identification Process (NDE); Federal Logistics Data (FED LOG); Logistics The Army Authorization Document System (LOGTAADS); Army Material Command Installation Supply System (AMCISS); Standard Army Retail Supply Level I (SARSS-1); Logistics Modernization Program (LMP); Base Operations Support System (BOSS); Defense Medical Logistics Supply System (DMLSS); Defense Automated Address System (DAAS); Contracting Officer Representative Administration System (CORAS); e-Biz; Defense Business Management System (DBMS); Standard Industrial Fund System (SIFS); Washington Allotment Accounting System (WAAS); Financial and Accounting Management Information System (FAMIS); Logistics Modernization Program (LMP); Defense Reutilization and Marketing Automated Information System (DAISY); Facility Equipment Management System (FEMS); Unique Item Tracking (UIT – CBS-X, DoDSASP, Cryptographic); Command Asset Visibility and Equipment Redistribution System (CAVERS); Integrated Facilities System (IFS); Planning Resource Infrastructure Decision Evaluation (PRIDE); and Portable Data Collection Device (PDCD) – internal interface

3.5. FINANCIAL STATEMENT AND LINE ITEMS SUPPORTED BY DPAS. DPAS provides financial reporting of capital assets and asset accountability and visibility for more than 10 million property assets valued at approximately $47 billion. DPAS provides standard general ledger accounting and subsidiary reporting for capital assets and tracks accountability for all types of property including personal property, real property, and heritage assets.

4.0 GUIDANCE/APPLICABLE DOCUMENTS

The contractor shall use the GAO FISCAM to develop the methodology and detailed audit steps to determine DPAS compliance with Business Management Modernization Program Systems Compliance Criteria, DITSCAP, the Federal Financial Management Improvement Act of 1996, the Federal Information Security Management Act, and SAS 70/88. 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), which 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 General Accounting Office (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. These standards, often referred to as Generally Accepted Government Auditing Standards (GAGAS), must be followed by auditors and audit organization when required by law, regulation, agreement, contract, or policy. 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.

5.0 AUDITS OF DOD FINANCIAL MANAGEMENT SYSTEMS

5.1. METHODOLOGY. The contractor shall perform an audit of DPAS using GAO FISCAM and SAS 70/88 guidance. This includes determining whether general and application controls are effective in design and operation and may be relied on to support CFO audit work. The contractor shall also assess whether DPAS complies with all relevant FFMIA requirements and other applicable laws and regulations and is properly certified and accredited in accordance with DITSCAP. Consistent with the GAO/PCIE Financial Audit Manual (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 GAO FAM and FISCAM.

5.2. DELIVERABLES. This task order includes the following deliverables for planning and internal controls, testing, and reporting phases. 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. Phase 1 of this task order applies only to developing the audit plan including a systems flow chart and test plan; oral presentations; providing a travel plan; and submitting written deliverables that are in conformity with guidance in Section 4.0, "Guidance/Applicable Documents." The contractor shall complete the following deliverables during the planning and internal controls phase.

5.2.1.1. KICKOFF AND ENTRANCE CONFERENCE. The contractor shall hold a kickoff 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 DPAS users and their auditors. 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. In compliance with applicable guidance, the contractor shall develop an audit plan to evaluate DPAS general and application controls, compliance, and certification and accreditation. The audit plan must include a risk assessment of the DPAS in accordance with DITSCAP. The plan must assess 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 be based on the GAO FISCAM 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 SAS 70/88 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 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."

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

5.2.1.5. ASSESS IHERENT 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 DPAS 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.

5.2.1.6. PRELIMINRY 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 primarily 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)

5.2.1.7. 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.

5.2.1.8. SYSTEM FLOW CHART. The contractor shall prepare a system flowchart for DPAS. The system flowchart shall describe the sequence of the key processes, manual operations, and inputs and outputs of the applications, as well as system interface details to include ownership and location of the systems interfaced.

5.2.1.9. TEST PLAN. The contractor shall include in the audit plan a test plan that delineates procedures to determine the extent of reliance on controls. 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. Further, the contractor shall determine whether the system complies with DITSCAP certification and accreditation. 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. The contractor shall perform tests of DPAS to determine whether general and application controls are properly designed and operating effectively, complies with all relevant FFMIA requirements and 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. The testing will include all system-related controls documented in the specific control evaluations worksheets (or similar documents) prepared during the planning and internal control phase. For controls the contractor determines are ineffectively designed or not operating as intended, the contractor must gather sufficient evidence to support appropriate findings and to provide recommendations to improve controls. The contractor shall complete the following deliverables during the testing phase.

5.2.2.1. SUMMARY MEMORANDUM. The contractor shall provide a summary memorandum separately documenting the tests of general controls, application controls, controls over the flow of DPAS data inputs and outputs, DPAS compliance with applicable laws and regulations, and DPAS certification and accreditation. The summary memoranda must include the results and conclusions related to the procedures performed, including condition, criteria, methodology, cause, effect, and recommended corrective actions. The COR will review and approve the summary memoranda.

5.2.2.2. 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.

5.2.2.3. PHASE III REPORTING. The contractor shall complete the following deliverables during the reporting phase. The Contractor shall be available for discussions and clarifications on issues in the reports and to perform edits to the reports until the reports have been finalized by the OIG.

For all reports, the Contractor shall ensure proper cross-reference to workpapers for each version submitted to the OIG for review and approval. The Contractor shall remain available to discuss and clarify issues in the report. Additionally, the Contractor shall be available to incorporate any required information into the report and provide written responses to questions concerning report language and audit recommendations.

DRAFT REPORT. The contractor shall provide a draft report no later than 30 days after the end of audit fieldwork. The draft report package will include a separate cross-referenced SAS 70/88 Type II report, a technical report, and an updated systems flow chart. The draft report must address the audit objectives in Section 2.0. The COR will review and approve the draft report package.

FINAL REPORT. The contractor will provide the IG DoD with a final audit report no later than 10 working days after receipt of IG DoD final comments on the draft report package. The final report package will include a separate cross-referenced SAS 70/88 Type II report, a technical report, and an updated systems flow chart. The COR will review and approve the final report package.

TECHNICAL REPORT. The technical report must conclude whether DPAS general and application controls and controls over DPAS data inputs and outputs are adequately designed and effective. The technical report must also conclude whether DPAS certification and accreditation complies with DITSCAP. 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 significant deficiency based on relevant standards. The

report will include an introduction, background, scope, methodology, overall summary of results, and a description of the system environment.

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.

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. 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 delivered working papers. The purpose of the training will be to facilitate the IG DoD and GAO review of the 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. 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. AUDIT STAFF. The contractor must submit a list of assigned auditors and their qualifications to the COR with the audit plan. The staff listing should include the security clearance of each individual. The COR shall approve all audit staff revisions.

6.3.3. SUB-CONTRACTOR INFORMATION. The prime contractor must provide, prior to contract award, 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 a travel plan 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 DPAS. In this separate statement, the contractor must briefly describe all work and known future work related to DPAS, including non-audit services 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 DPAS. 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 monthly 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 DPAS 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-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. To evaluate proposals submitted, each bidder shall submit a Statement of Independence and a list of prior clients we can contact to discuss their opinion on the quality of the bidder's prior work.

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 the audits.

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.

Deliverables:	Due Date:
List of Key Personnel (to PCO)	At contract award
List of Assigned Auditors (to COR)	15 days from issuance of Task Order
Subcontractor Information	Prior to contract award
Statement of Independence	Prior to proposal submission
Non Disclosure Agreement	Prior to start of work
Audit Plan	Draft Due within 60 days from award date Final Due one week after final COR Comments
System Flow Chart	With audit plan
Test Plan	Draft Due with audit plan Final Due one week after final COR Comments
Kickoff meeting and Entrance Conference	TBD
In Process Reviews (2)	Completion of Planning Phase and TBD
Summary Memorandum	TBD
Progress Report	Monthly
Exit Conference	TBD
All Audit Documentation	With Draft Audit Report Package
Draft Audit Report Package including:	Within 30 days from end of Field Work
Cross-referenced Audit Report	
Technical Report	
Remediation Plan (if applicable)	
Updated System Flow Chart	
Management Letter (if applicable)	
Final Audit Report Package including:	TBD
Final cross referenced Audit Report	
Final Technical Report	
Final Remediation Plan (if applicable)	
Final Management Letter (if applicable)	
Travel Plan	No later than 10 work days prior to travel
Other Direct Costs	Prior to incurring cost
Contractor Proposal on other work involving Component	Prior to contract proposal on other work involving Component
Material findings	Within 24 hours