Review of Management of the Department's Certification and Accreditation Contract

FINAL AUDIT REPORT

ED-OIG/S19-E0015
December 2004

Our mission is to promote the efficiency, effectiveness, and integrity of the Department's programs and operations.

U.S. Department of Education
Office of Inspector General
Operations Internal Audit Team
Washington, DC

Statements that managerial practices need improvements, as well as other conclusions and recommendations in this report, represent the opinions of the Office of Inspector General. Determinations of corrective action to be taken will be made by the appropriate Department of Education officials.

In accordance with the Freedom of Information Act (5 U.S.C. § 552), reports issued by the Office of Inspector General are available to members of the press and general public to the extent information contained therein is not subject to exemptions in the Act.

UNITED STATES DEPARTMENT OF EDUCATION

OFFICE OF INSPECTOR GENERAL

December 17, 2004

MEMORANDUM

TO: Edward R. McPherson
Under Secretary for Education

FROM: Thomas A. Carter /s/
Deputy Inspector General
Office of Inspector General

SUBJECT: Final Audit Report
Management of the Department's Certification and Accreditation Contract
Control Number ED-OIG/S19-E0015

Attached is the subject final audit report that covers the results of our review of the management of the Department's Certification and Accreditation contract during the period June 2003 through December 2003. An electronic copy has also been provided to the Chief Financial Officer, the Assistant Secretary for Management and Chief Information Officer, and their Audit Liaison Officers. We received comments to our draft report from the Office of the Chief Financial Officer (OCFO) and the Office of the Chief Information Officer (OCIO) generally non-concurring with the findings, but generally concurring with the recommendations. No changes were made to the report as a result of the Department's comments. We are issuing this report to you since it contains cross-cutting issues in both OCFO and OCIO.

Corrective actions proposed (resolution phase) and implemented (closure phase) by your offices will be monitored and tracked through the Department's Audit Accountability and Resolution Tracking System. Department policy requires that you develop a final corrective action plan (CAP) for our review in the automated system within 30 days of the issuance of this report. The CAP should set forth the specific action items, and targeted completion dates, necessary to implement final corrective actions on the findings and recommendations included in this final audit report.

In accordance with the Inspector General Act of 1978, as amended, the Office of Inspector General is required to report to Congress twice a year on the audits that remain unresolved six months after the date of issuance.

In accordance with the Freedom of Information Act (5 U.S.C. §552), reports issued by the Office of Inspector General are available to members of the press and general public to the extent information contained therein is not subject to exemptions in the Act.

We appreciate the cooperation given us during the review. If you have any questions, please call Michele Weaver-Dugan at (202) 245-6941.

cc: Jack Martin, Chief Financial Officer
William Leidinger, Assistant Secretary for Management and Chief Information Officer

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The National Institute of Standards and Technology states, "Security certification and accreditation are important activities that support a risk management process and are an integral part of an agency's information security program." The Department of Education (Department) established a contract to acquire technical support for its certification and accreditation (C&A) program. The C&A contract included three primary requirements that its information systems would be subjected to – a documentation review, security test and evaluation (ST&E), and, for select systems, vulnerability scanning and penetration testing.

The objective of our audit was to determine the effectiveness of the Department's management of the C&A contract. Our audit was limited to the review of deliverables related to the documentation review and vulnerability scanning/penetration testing requirements of the contract for the initial 10 Tier 4 systems subjected to the C&A process. (See Attachment 1 for further information on Tier 4 systems and the 10 systems included in our review.) The Office of Inspector General (OIG) reviewed the ST&E requirements under a separate project and issued the results of that review separately. [1]

Overall, we found that Department staff did not effectively manage the C&A contract and that improvements were needed in the Department's contract management process. Department staff did not adequately track and inspect deliverables, gave unauthorized instructions to the contractor to reduce the scope of work to be performed, did not inform the Contracting Officer (CO) of changes in key personnel, and did not document evaluations of contractor-submitted reports. As a result, the Department paid for deliverables that were not provided or that did not meet acceptance criteria, and improperly authorized incentive payments to the contractor. A subsequent modification to the contract was issued, in part to correct the work that was not adequately performed, resulting in the Department paying twice for the same required services. We also found the Performance Work Statement (PWS) for the C&A contract did not require sufficient documentation to support C&A recommendations and decisions. The C&A services initially received did not provide managers with complete, supportable information upon which to base their certification decisions.

To correct the weaknesses we identified, we recommended that the Department:

- Ensure that the staff member assigned as the Contracting Officer's Representative (COR) is provided sufficient resources to fulfill his/her responsibility for overall contract monitoring, and that other involved staff provide the COR with appropriate input as needed. Specifically, a contract monitoring plan should be developed to ensure that all aspects of the contract are appropriately monitored and Department policies are followed.

[1] Audit Control Number, A11-E0002, "Department of Education's Implementation of [Federal Information Security Management Act] FISMA, Fiscal Year 2004," dated October 6, 2004.

- Ensure the CO, COR, and other staff and contractors involved in contract management, meet to review the contract monitoring plan and agree upon the methodology for monitoring the remainder of this contract. Ensure all parties understand their responsibilities for contract monitoring.
- Require the contractor to formally request substitution of key personnel already removed from the contract, and for any future substitutions, including submitting resumes for evaluation by the Department to ensure the level of expertise is comparable to the original key personnel.
- Ensure the CO provides any subsequent CORs with memoranda to outline responsibilities and limitations as required by the Department Directive, and provides notice to the contractor of any change in CORs.
- Obtain an Office of General Counsel (OGC) opinion regarding possible remedies to recover funds from the contractor for improper incentive payments, unacceptable deliverables, and reductions to the scope of work made without the authorization of the CO. If indicated by the opinion, pursue recovery of funds from the contractor.
- Review the current PWS and ensure that sufficient documentation is required to support C&A recommendations and decisions.
- Ensure that all future PWS for C&A contracts include requirements for documentation supporting scans, tests, and analyses conducted, and decisions made on the risks and mitigating factors considered, in support of the contractor's C&A recommendations.

The Department initially provided a response to our draft report on October 4, 2004. The Department retracted that response on October 7, 2004. An amended response was provided on October 12, 2004. The Department retracted that response on October 14, 2004. The final response was provided on October 18, 2004, and that is the document we refer to as the "Department's response." Some information in the Department's response conflicted with information provided to us by Department officials during our review.

In its response, the Department stated,

> . . .[W]hile acknowledging that contract related processes early in the C&A contract period could have been performed to more closely adhere to the Department's contract procedures and policies, the Department does not concur in whole, with the findings of the draft audit. The Department believes that the C&A contractor's performance met the objectives of the contract in support of the C&A program.

The Department did not concur in whole with the findings, but it did concur with six of the seven recommendations made. The Department did not concur with the recommendation to obtain an OGC opinion regarding possible remedies to recover funds from the contractor.

OIG's position has not changed on the issues reported in the findings, or on the recommendations made. No changes were made to the report as a result of the Department's responses.

In Attachment 3, we have provided comments to the Department's response. The Department's response is included in its entirety as Attachment 4 to this report.

Throughout the review, OIG experienced delays in obtaining information from Department staff. Office of the Chief Information Officer (OCIO) staff had difficulty locating deliverables, and/or determining what documents, if any, the contractor provided to satisfy deliverable requirements. OCIO files were not complete and did not include evidence of inspection and acceptance or rejection of deliverables. Some deliverables that the Department stated were provided could not be located. OCIO staff reported that a number of verbal agreements were made with the contractor regarding the scope of work, but no documentation existed to support any of these agreements.

The conflicting information and multiple responses to our draft report from the Department, along with our difficulties in obtaining information, indicate a lack of familiarity with contract requirements and with work actually accomplished. This supports our conclusion that the Department did not effectively manage the contract. It also lessens the Department's credibility with regard to any statements provided by Department management and staff, especially in the absence of supporting documentation. As a result, we were presented with a scope limitation in that we were unable to determine whether the vulnerability scans performed as part of the C&A effort resulted in any findings that should have been reported to management. As such, we were not able to conclude whether deliverables regarding vulnerability scanning and penetration testing should have been provided by the contractor.

BACKGROUND

The National Institute of Standards and Technology (NIST), Special Publication 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems," states:

> Security certification and accreditation are important activities that support a risk management process and are an integral part of an agency's information security program. Security accreditation is the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations, agency assets, or individuals based on the implementation of an agreed-upon set of security controls. Required by OMB [Office of Management and Budget] Circular A-130, Appendix III, security accreditation provides a form of quality control and challenges managers and technical staffs at all levels to implement the most effective security controls possible in an information system, given mission requirements, technical constraints, operational constraints, and cost/schedule constraints. By accrediting an information system, an agency official accepts responsibility for the security of the system and is fully accountable for any adverse impacts to the agency if a breach of security occurs. Thus, responsibility and accountability are core principles that characterize security accreditation.

The Department of Education (Department) established a contract to acquire technical support for its certification and accreditation (C&A) program. The Performance Work Statement (PWS) for the contract included the following as responsibilities of the contractor:

- Reviewing and evaluating system security documentation to ensure it is complete and complies with Department policies and guidelines,
- Conducting security test and evaluation (ST&E), and vulnerability and penetration tests, if applicable,
- Documenting test findings,
- Providing system owner out briefs,
- Writing a summary report of certification activities performed and their results,
- Justifying the certification recommendation,
- Briefing the certifier on the review findings and the certification recommendation, and
- Supporting recertification and revalidation.

The original contract, effective June 25, 2003, included requirements to complete C&A services for 25 systems by December 31, 2003. Included in these systems were 10 Tier 4 systems – the highest risk systems in the Department. (See Attachment 1 for further information on Tier 4 systems and the 10 systems included in our review.)

The C&A contract included three primary requirements for the Tier 4 systems – documentation review, ST&E, and vulnerability scanning and penetration testing. Our audit was limited to analysis of contract management for the documentation review and vulnerability scanning/penetration testing requirements of the contract for the 10 original Tier 4 systems. The Office of Inspector General (OIG) is reviewed the ST&E requirements under a separate project and issued the results of that review separately. [2]

The Department originally awarded the contract for $1,026,311, including incentives, for 25 systems. This amount included $437,400 for 10 Tier 4 systems. The Department issued modifications to the contract to exercise option years, add additional 35 systems to the C&A process, and for other related services, bringing the total contract amount to $2,842,367, as of January 5, 2004.

Subsequent to the start of our audit work, effective July 13, 2004, the Department issued Modification 0005 to the C&A contract to recertify and accredit, or validate the existing certification and accreditation, of 60 systems, including the original 10 Tier 4 systems that were the subject of our review. Under this modification, the work to be performed for these Tier 4 systems was primarily for vulnerability scanning and penetration testing, and a final security assessment report. The total value of this modification for the original 10 Tier 4 systems was $253,692.[3] The total contract amount through Modification 0005 was $3,172,486.

[2] Audit Control Number, A11-E0002, "Department of Education's Implementation of [Federal Information Security Management Act] FISMA, Fiscal Year 2004," dated October 6, 2004.

[3] The modification for the original 10 Tier 4 systems also included additional C&A services for 3 of the 10 systems that the modification stated experienced significant changes since the last C&A review. For these three systems, the modification also included deliverables for C&A documentation reviews, and ST&E execution and documentation.

AUDIT RESULTS

We found Department staff did not effectively manage the C&A contract. Department staff did not adequately track and inspect deliverables, gave unauthorized instructions to the contractor to reduce the scope of work to be performed, did not inform the Contracting Officer (CO) of changes in key personnel, and did not document evaluations of contractor-submitted reports. As a result, the Department paid for deliverables that were not provided or that did not meet acceptance criteria, and improperly authorized incentive payments to the contractor. A subsequent modification to the contract was issued, resulting in the Department paying twice for the same services. We also found the PWS for the C&A contract did not require sufficient documentation to support C&A recommendations and decisions. The C&A services initially received did not provide managers with complete, supportable information upon which to base their certification decisions.

In its response, the Department stated,

> . . .[W]hile acknowledging that contract related processes early in the C&A contract period could have been performed to more closely adhere to the Department's contract procedures and policies, the Department does not concur in whole, with the findings of the draft audit. The Department believes that the C&A contractor's performance met the objectives of the contract in support of the C&A program.

The Department did not concur in whole with the findings, but it did concur with six of the seven recommendations made. OIG's position has not changed on the issues reported in the findings, or on the recommendations made. No changes were made to the report as a result of the Department's response. (See Attachment 3 for comments by OIG to the Department's response, and Attachment 4 for a copy of the Department's response.)

Finding No. 1 – Department Staff Did Not Effectively Manage the C&A Contract

Department staff did not effectively manage the contract for C&A services. Specifically, we found that the Contracting Officer's Representative (COR), and other Office of the Chief Information Officer (OCIO) staff and contractors involved in contract monitoring:

a. Did not adequately track and inspect deliverables to ensure that contract requirements were met. We found that some deliverables were not provided, and others did not meet acceptance criteria provided in the contract.

b. Gave unauthorized instructions to the contractor to reduce the scope of work to be performed.
c. Did not ensure that the CO was informed of changes in key personnel and that the contractor submitted to the CO formal notice and requests for written approval of substitution of key personnel.
d. Did not document evaluations of contractor-submitted reports or provide written evaluations of the reports to the CO.

Federal Acquisition Regulation (FAR) Part 37, "Service Contracting," § 37.102(h), states, "Agencies shall ensure that sufficiently trained and experienced officials are available within the agency to manage and oversee the contract administration function." FAR § 37.114, "Special Acquisition Requirements," states:

> Contracts for services which require the contractor to provide advice, opinions, recommendations, ideas, reports, analyses, or other work products have the potential for influencing the authority, accountability, and responsibilities of Government officials. These contracts require special management attention to ensure that they do not result in performance of inherently governmental functions by the contractor and that Government officials properly exercise their authority. Agencies must ensure that-
>
> (a) A sufficient number of qualified Government employees are assigned to oversee contractor activities, especially those that involve support of Government policy or decision making. . ..
>
> (b) A greater scrutiny and an appropriate enhanced degree of management oversight is exercised when contracting for functions that are not inherently governmental but closely support the performance of inherently governmental functions. . ..

The Department's Administrative Communication System Directive (Directive), Office of the Chief Financial Officer (OCFO):2-108, "Contract Monitoring for Program Officials," dated January 12, 1987,[4] Section I, states that the purpose of the Directive is to provide internal standards and guidelines for monitoring of contracts by program officials. Included in the Directive are specific guidelines for inspection and acceptance, documenting and maintaining monitoring information, evaluating reports provided by the contractor, and ensuring the CO is informed of important issues related to contractor performance, including changes in key personnel.

Section II of the Directive states:

> It is the policy of the Department of Education (a) to monitor every contract to the extent appropriate to provide reasonable assurance that the contractor performs

[4] The Department updated and reissued this Directive on April 15, 2004. The requirements presented above from the former policy (in effect during the scope of our review) are also presented in the updated policy.

the work called for in the contract, and (b) to develop a clear record of that performance and the Department's efforts in monitoring it.

Section VIII.A of the Directive states, "Contract monitoring is conducted by the Government to ensure that the contractor performs according to the specific promises and agreements that make up the contract."

a. The COR, other OCIO staff, and the project management contractor, did not adequately track and inspect deliverables to ensure that contract requirements were met.

We found that some deliverables were not provided, and others did not meet the acceptance criteria provided in the contract. Specifically, we found:

- Deliverables regarding rules of engagement for vulnerability scans/penetration testing, evidence that vulnerability scans/penetration testing were conducted, and minutes for system owner and certifier out briefs were not provided.
- Matrices of observations, vulnerability scans/penetration testing reports, system owner out briefs, and certifier out briefs deliverables were not complete and did not meet acceptance criteria.
- The contractor did not report on whether issues noted in the 2002 risk assessments had been mitigated as required by the contract.
- Issues reported in the matrices of observations were not consistent with issues reported in the system owner and certifier out briefs.

See Attachment 2 for details on results by deliverable.

The FAR states that the Government has the right to inspect and test all services. If any services do not conform to contract requirements, the Government may require the contractor to perform the services again at no increase to the contract amount (FAR § 52.246-4(e)). The FAR also prescribes policies and procedures to ensure supplies and services conform to requirements. Acceptance is defined as acknowledgment that services/deliverables conform to applicable contract quality and quantity requirements (FAR § 46.501). Acceptance ordinarily is evidenced by execution of an acceptance certificate on an inspection or receiving report form (FAR § 46.501).

Department policies require that for deliverables sent to the COR, the COR is generally responsible for conducting the inspection and, depending on the contract, for making acceptance or for recommending to the CO whether acceptance should be made. The COR's decision to accept deliverables or to recommend their rejection must be furnished in writing to the CO using a receiving report or receipt, (Directive OCFO 2-108, Sections XI.A.1 and XI.B.1). Receipts are provided electronically through the Department's Contract and Purchasing Support System. Department policy also states that constructive acceptance occurs seven days after delivery of supplies or services. For service contracts, Department policy requires that receipts be provided when invoices are received, (OCFO Procedures that Work, CO-008).

We found that deliverables were not adequately tracked and inspected because:

- OCIO fragmented responsibility for contract management between the COR, other OCIO staff, and a contractor hired for project management,
- Monitoring focused on schedules, not deliverables,
- The Department's receipts process for service contracts does not document acceptance of deliverables.

OCIO Fragmented Contract Management Responsibilities

We found that the COR, other OCIO staff, and the project management contractor, did not adequately track and inspect deliverables because the program office fragmented the responsibility for monitoring contract performance. The COR responsible for the contract between September 2003 and April 2004 stated that she was not a technical expert in the area, and was not able to devote a great deal of time to this contract as she was also assigned other tasks. OCIO hired another contractor to perform project management for the C&A process. Department policy states that the COR is responsible for monitoring the programmatic or technical aspects of a contract and making recommendations to the CO for necessary contract administration actions, including the inspection and acceptance of deliverables. These duties, however, were spread among other OCIO staff members and a project management contractor, making it difficult for the COR to manage several individuals that were performing parts of the COR's duties. Other OCIO staff members and the project management contractor had also not received the Department's contract monitoring training and as such, may not have been familiar with contract monitoring requirements.

Monitoring Focused on Schedules, Not Deliverables

The project tracking by the COR, other OCIO staff, and the project management contractor centered on monitoring schedules and did not include detailed inspection of deliverables for compliance with the quantity and quality requirements of the contract. In fact, OCIO staff responsible for monitoring the contract were not familiar with all deliverable requirements. For example, we found the COR and other OCIO staff were not familiar with the requirement that minutes of the out briefs be recorded and distributed. OCIO staff were not familiar with which systems received penetration testing. OCIO staff also did not realize that the out brief deliverables did not consistently include information on vulnerability scans and penetration testing. An OCIO staff member stated that the vulnerability scans and penetration tests were discussed verbally in the out briefs, however, since no minutes were provided, no documentation exists to support the discussions.

Receipts Process for Service Contracts Does Not Document Acceptance of Deliverables

In addition, because the Department's process for indicating receipt is based on invoices rather than deliverables, no formal, written acceptance of individual deliverables was made. Progress payments were authorized under the contract based on a monthly allocation of total contract costs. The COR stated that she matched the invoice amounts to the schedule. The COR stated that she did not inspect deliverables, but provided them to other OCIO staff with technical expertise. Receipts from the COR included general statements about progress on the contract, rather than any indication that deliverables received to date were inspected and accepted. Through Modification 0005 to the contract, the Department aligned the receipts process with deliverables for this contract. The modification states, "The contractor shall invoice on a monthly basis only for the deliverables received and accepted by the Department."

As a result, the Department paid for deliverables that were not provided, or for deliverables that did not meet contract acceptance criteria. Without complete information on the penetration risk level included in the out briefs, or a statement that there were no risks in this area, the certifying official did not have complete information upon which to base the certification decision. Constructive acceptance has already occurred since more than seven days have elapsed from receipt of these deliverables. As such, the Department may have lost the opportunity to require that the contractor correct the deficiencies noted without additional cost to the Government.

In addition, the contractor was improperly paid a total of $83,622 in performance incentives for work during the initial contract period. Contract terms stated that the incentives would be paid only if all deliverables meet the acceptance criteria and due dates specified. Since not all deliverables were provided, and some deliverables were not complete and therefore did not meet acceptance criteria, the contractor should not have been paid any of the incentive amounts.

b. OCIO staff gave unauthorized instructions to the contractor to reduce the scope work to be performed.

During performance, OCIO clarified contract requirements, and reduced the scope of work for vulnerability scans and penetration testing, without proper authority to do so. OCIO staff did not formalize these changes to the contractor in writing, nor was the CO informed of these changes.

Specifically we noted:

- OCIO staff clarified what would be considered a "finding" for vulnerability scans.
- The contractor responsible for the operation of the Common Origination and Disbursement (COD) system, and that contractor's auditors, performed the vulnerability scans and penetration testing for that system, rather than the C&A contractor as required by the contract.
- The contractor responsible for the operation of the Direct Loan Servicing System (DLSS) performed the vulnerability scans for that system, rather than the C&A contractor as required by the contract.

- The contract called for penetration testing to be performed for all 10 Tier 4 systems. However, agreement was reached between the Department and the C&A contractor that penetration testing would not be performed if there was a chance that systems would be disrupted. As a result, the C&A contractor did not perform penetration testing for any of the 10 Tier 4 systems. (Only the COD system received penetration testing, as discussed above.)
- OCIO staff and the contractor agreed that the Certification Recommendations Report deliverables specified in the contract for each system were not required. OCIO staff considered the certifier briefing to satisfy the requirements for this deliverable, even though all required areas of the deliverable were not included in the certifier briefing.

Neither OCIO staff nor the contractor could provide electronic mail messages or other documentation that discussed the specifics of these changes and the agreement of the parties to the changes.

The CO is the only Department official authorized to make changes to the contract. The COR is not authorized to modify or change the terms of the contract, such as obligated cost or price, delivery, or scope of work. Department policy states that the CO relies on the COR for collecting monitoring information and making related analyses and recommendations for administrative action. This information and analysis must be fully documented and reported promptly to the CO so that the Government's interests can be protected, and so that the program office will have the facts upon which to make informed decisions about the contract and the program in general, (Directive OCFO:2-108, Section IX.C.2).

Department policy further states that the Government's record for a contract is maintained primarily in two places: In the program office, and in the contracting office. The program office file, maintained by the COR, should contain all information needed by the COR to carry out his or her contract monitoring and managing responsibilities. The file maintained by the CO is the Government's "official file" and must contain all information having even the slightest bearing on the obligations of the two parties to the contract and their performance against those obligations, (Directive OCFO:2-108, Section IX.D.5).

Department Directive OCFO:2-108, Section IX.N, states:

1. The purpose of detailed record-keeping is to build a complete history of each project so that information is not lost or forgotten, and so that others – e.g. one's supervisor, a new COR assigned to the project, and auditor, or perhaps a court of law – can get a clear picture of what has occurred during the life of a contract. (If a dispute occurs, it could be several years between the event and its resolution. The COR and program office files could be called upon at a very late date.)
2. As a general rule, the COR should document every significant action taken or conversation held in the course of monitoring or administering a contract.

The COR and OCIO staff did not obtain CO approval for the clarifications and changes made in requirements for the contractor's performance. As a result, the CO was not aware of the

changes, and was not able to evaluate the impact of those changes on the scope of work in the contract, including determining whether the contract price should be reduced. Fragmentation of contract monitoring responsibilities, as previously discussed, may have contributed to the issues noted. While all CORs assigned to the contract had completed certification training, other OCIO staff heavily involved in contract management, and the project management contractor, may not have been familiar with or did not follow Department policies and procedures on communication with the CO and contract file documentation. The CO did not provide the first two CORs on the project with letters delegating authority for contract monitoring responsibilities. As such, these CORs may not have fully understood their responsibilities and/or the extent and limitation of their authority.[5]

Verbal agreements on the definition of a finding for vulnerability scans, and reductions to the scope of work for vulnerability scans, penetration testing, and other deliverables, could later lead to disputes if one party's recall of the discussion or agreements differs from the others. The changes related to vulnerability scans and penetration testing, and elimination of the certification recommendation report, resulted in a decreased level of effort by the contractor and should have resulted in a modification and a decrease in the contract price to reflect the work originally required by the contract that was not performed.

In addition, the informal agreement regarding the extent of penetration testing for the Tier 4 systems resulted in less assurance for the Department that these high-risk systems were adequately protected against unauthorized access.

c. The COR/OCIO staff did not ensure that the CO was informed of changes in key personnel and that the contractor submitted to the CO formal notice and requests for written approval of substitution of key personnel.

During contract performance, two of the four key personnel designated in the contract – both of the designated team leaders – were removed from the contract. One team leader was removed after two months of contract performance because he failed to meet the requirements of the Department's security clearance process. The other team leader was promoted within the contractor's organization and removed from the C&A project after six months of performance. The contractor did not submit substitutions of key personnel for approval by the CO as required. Section H.1 of the C&A contract states that,

> The personnel designated as key personnel are considered to be essential to the work being performed hereunder. Prior to diverting any of the specified individuals to other programs, or otherwise substituting any other personnel for specified personnel, the contractor shall notify the Contracting Officer and the COR reasonably in advance and shall submit justification (including proposed substitutions) in sufficient detail to permit evaluation of the impact on the task

[5] The initially assigned COR was responsible for contract monitoring from the start of the contract in June 2003, until his departure from the Department in September 2003. The second COR was responsible for contract monitoring from September 2003, until her departure from the Department in April 2004. The current COR has been assigned to the contract since April 2004.

> order effort. No diversion or substitution shall be made without the written consent of the contracting officer. . .The task order will be modified to reflect the addition or deletion of key personnel.

Directive OCFO:2-108, Appendix F, "Checklist of Questions to Consider When Monitoring," includes the following:

- Are key personnel performing under the contract to the extent agreed to?
- Has the contractor notified the Government of any changes to the key personnel?

This section further states, "If the answer to any of the preceding questions was "NO," has the ED [Department] Contracting Officer been notified so that prompt corrective action may be taken?"

The COR and other OCIO staff were aware that the key personnel had been removed from the contract. However, the COR did not follow Department policies by ensuring that the contractor complied with contract terms and notified and provided information on substitute personnel to the CO for evaluation.

As a result, the expertise and level of knowledge of the personnel substituted may not have equaled that of the designated key personnel upon which the contract award decision was at least partially based. The level of service provided might have been less than what was originally purchased. The purpose of the contract, as stated in the PWS, was to ". . .acquire expert technical support. . .." Without evaluation of the personnel substituted for the experts originally hired, the Department does not have the same level of assurance in the quality of the services it received.

d. The COR did not document evaluations of contractor-submitted reports or provide written evaluations of the reports to the CO.

The contract included requirements for reports in addition to the deliverables for the C&A process. These reports included:

- Weekly status reports on the overall implementation and status of the entire process,
- Project plans for each system including personnel assigned, proposed schedule and cost estimates, and
- Monthly earned value management reports for each system.

We found, however, there was no documentation to indicate whether the COR reviewed and made written evaluations of these reports, or provided those evaluations to the CO.

Department policy states that the COR must promptly read all progress reports submitted by the contractor. Failure to read the reports negates their considerable value in keeping the Government up to date. The COR must make a written evaluation of each report. Depending on the type of contract and relative importance of the report, the evaluation might be either rigorous

or reasonably informal. All evaluations of reports should be sent to the CO. The COR must ensure that copies of reports and the evaluations made of them are entered in the program office file, (Directive OCFO:2-108, Sections X.D.2.a and c, X.D.4.b and d).

The COR or other OCIO staff did not follow Department requirements to promptly read and document evaluations of reports submitted by the contractor. As previously mentioned, the COR stated that she had other responsibilities and was not able to devote a great deal of time to this contract.

As a result, potential problem indicators included in the reports may not have been detected by the COR. In addition, the CO was not provided evaluations to confirm that reports were being received as required by the contract, and to indicate any potential problems so that the CO could promptly take any required action to protect the Government's interests.

Summary

Without an effective flow of information between the CO and COR, the CO cannot ensure the COR is adequately performing the contract monitoring tasks they have been delegated, nor can the CO ensure that contract progress is satisfactory.

Program staff who are unfamiliar with contract terms, deliverable requirements, or regulations, policies and procedures to be followed in monitoring contracts, are unable to achieve the basic purpose of contract monitoring – to provide reasonable assurance that the contractor performs work called for in the contract. Inadequate documentation of contract monitoring, contract changes, and review and acceptance of deliverables, impairs the Department's ability to hold the contractor accountable for performance. Failure to enforce contract terms may also constitute a waiver of the Department's rights to enforce contract terms, may support interpretations of contract requirements contrary to the Government's best interest, and/or may subsequently weaken the Government's position to effectively defend itself in contract disputes.

Unauthorized agreements to reduce the work to be performed and deliverables to be provided under the contract reduced the assurance the Department could place in the C&A process and in the security of its systems. Since the contract price was not modified to reflect the reduction in effort, the Department paid for work that was not performed.

Subsequent to the start of our audit work, effective July 13, 2004, the Department issued Modification 0005 to the C&A contract to recertify and accredit, or validate the existing certification and accreditation, of 60 systems, including the original 10 Tier 4 systems that were the subject of our review. For the original 10 Tier 4 systems, Modification 0005 included requirements to repeat the vulnerability scans and penetration testing included in the original contract for these systems. The modification also included a final security assessment report for the original 10 Tier 4 systems. This report included essentially the same acceptance criteria as were included for the certification recommendation report that OCIO staff determined was not needed. In total, Modification 0005 included $243,692 for the 10 Tier 4 systems. Of this amount, $122,472 was to repeat C&A analyses and documentation that should have been

completed under the initial contract for seven of the systems, and $131,220 was for C&A services on three systems that the modification stated had experienced significant changes since the original C&A review. As a result of the weaknesses in contract management, the Department will be paying for many of the C&A services twice.

Recommendations:

We recommend that the Chief Financial Officer, in conjunction with the Assistant Secretary for Management and Chief Information Officer, take action to:

1.1 Ensure that the staff member assigned as COR has the technical knowledge required and is provided sufficient resources to fulfill his/her responsibility for overall contract monitoring, and that other involved staff provide the COR with appropriate input as needed. Specifically, a contract monitoring plan should be developed by which the COR ensures:

a. Deliverables are tracked, inspected in accordance with contract requirements, and formally accepted or rejected;
b. The CO is involved in all discussions regarding changes to the scope of work, and provides appropriate authorization for any such changes,
c. The CO is notified of changes in key personnel;
d. Evaluations of contractor reports are documented and provided to the CO; and
e. Contract file documentation includes all information needed to carry out his/her monitoring and managing responsibilities in accordance with Department policy.

1.2 Ensure the CO, COR, and other OCIO staff and contractors involved in contract management, meet to review the contract monitoring plan, and agree upon the methodology for monitoring the remainder of this contract. During the meeting, the CO should review the requirements in the FAR, the Department's Directive for contract monitoring, and the terms of the contract, including deliverable requirements, to ensure that all parties understand their responsibilities for contract monitoring.

1.3 Require the contractor to formally request substitution of key personnel already removed from the contract, and for any future substitutions, including submitting resumes for evaluation by the Department to ensure the level of expertise is comparable to the original key personnel.

1.4 Ensure the CO provides any subsequent CORs with memoranda to outline responsibilities and limitations as required by the Department Directive, and provides notice to the contractor of any change in CORs.

1.5 Obtain an Office of General Counsel (OGC) opinion regarding possible remedies to recover funds from the contractor for improper incentive payments, unacceptable deliverables, and reductions to the scope of work made without the authorization of the CO. If indicated by the opinion, pursue recovery of funds from the contractor.

Department Response

The Department did not concur in whole with the finding, and concurred with four of the five recommendations for this finding. The Department did not concur with the last recommendation above, and stated in its response,

> The Department does not concur that incentive payments were made to the contractor improperly, that deliverables were unacceptable, or that payment was made for more than it should have for the work completed. The Contracting Officer had already determined that an opinion is not required from Office of General Counsel.

OIG Comments

OIG continues to recommend that OGC be consulted for an opinion on this matter. (See Attachment 3 for detailed comments to the Department's response.)

Finding No. 2 – The Performance Work Statement Did Not Explicitly Require Sufficient Documentation to Support C&A Recommendations and Decisions

We found that the PWS did not explicitly require the contractor to provide or maintain supporting documentation of decisions made during the C&A process to support the contractor's C&A recommendations and therefore the Department's certification decisions. Deliverables submitted included briefing slides or summaries that did not provide information on the initial issues noted and resolved during the C&A process. The Department therefore received very little information to support the decisions and recommendations made by the contractor.

In addition, as discussed in Finding 1, OCIO and the contractor agreed to changes that reduced the scope of work and deliverables required under the contract. These changes further reduced the documentation provided to support decisions made in the C&A process.

NIST Special Publication 800-37, Executive Summary, states:

> It is essential that agency officials have the most complete, accurate, and trustworthy information possible on the security status of their information systems in order to make timely, credible, risk-based decisions on whether to authorize operation of those systems. The information and supporting evidence needed for security accreditation is developed during a detailed security review of an information system, typically referred to as security *certification*. Security certification is a comprehensive assessment of the management, operational, and

> technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. The results of a security certification are used to reassess the risks and update the system security plan, thus providing the factual basis for an authorizing official to render a security accreditation decision.

NIST 800-37, Section 1.1, states:

> The purpose of this publication is to provide guidelines for the security certification and accreditation of information systems supporting the executive agencies of the federal government. The guidelines have been developed to help achieve more secure information systems within the federal government by:
>
> - Enabling more consistent, comparable, and repeatable assessments of security controls in federal information systems;
> - Promoting a better understanding of agency-related mission risks resulting from the operation of information systems; and
> - Creating more complete, reliable, and trustworthy information for authorizing officials—to facilitate more informed security accreditation decisions.

NIST 800-37, Section 2.2, allows the delegation of certification and accreditation roles to qualified individuals, including contractors, with the exception of the roles of the Chief Information Officer and authorizing official. The delegated roles can include the determination of risk to agency operations. The only activities that must be performed by the authorizing official (i.e. government employee), is the actual security accreditation decision and the signing of the accreditation letter. However, agency officials retain ultimate responsibility for the results of actions performed by individuals in delegated roles.

Department staff stated that the intent of the contract was to purchase the contractor's expertise in conducting the C&A process. At one point, the contractor offered the Department raw data obtained during performance of the contract, and upon which its recommendations were based, but Department officials did not want the information stating they had no one qualified to review it. Based on OIG's inquiries related to this and other reviews, the contractor later provided the Department with its vulnerability scans for 7 of the 10 Tier 4 systems, but other information developed in its analyses to support the certification recommendations had been destroyed as the Department did not want the data and there was no requirement to maintain it. As a result, we could find no information to support the decisions made by the contractor and its certification recommendation to the Department.

Since detailed information was not submitted, the Department may not be fully aware of what vulnerabilities were noted and corrected prior to the completion of the C&A process. In fact, when questioned as part of this review, neither the Department nor the contractor could initially provide information as to which systems, if any, received penetration testing as part of the C&A

process. Information on the issues or vulnerabilities, and the actions taken to correct them, would be helpful to the Department in avoiding similar mistakes in the future, as well as providing information on the performance of system managers or other contractors responsible for the security and operation of the Department's systems. Detailed information on the C&A process and results could allow Department staff conducting C&A reviews in the future to evaluate the work performed by this contractor and build on that to identify recurring problems or improvements that have been made. The Department missed a significant opportunity to obtain management information by not requiring the contractor to provide full documentation of the analyses and decisions made in the process.

The information provided by the C&A contractor does not meet the purpose of the NIST guidance – to help achieve more secure information systems by (1) enabling consistent, comparable and repeatable assessments, (2) promoting a better understanding of risks, and (3) creating more complete, reliable and trustworthy information to facilitate more informed security accreditation decisions. With only the very limited information provided by the contractor, the Department is not able to satisfy these requirements.

The Department should review the appropriateness of the decisions made by the contractor in order to ensure that the work performed by the contractor was thorough and complete and met the objectives of the Department's C&A process and the requirements of the contract. Since the Department had not previously dealt with this contractor, it was not justified in placing a high amount of trust in an unknown source.

Effective July 13, 2004, the Department recently modified the C&A contract to recertify and accredit, or validate the existing certification and accreditation, of many systems, including all of the 10 Tier 4 systems reviewed. The modified PWS required additional documentation and reports that represent an improvement over the prior PWS. However, as noted in Finding 1, significant improvement in contract management is needed to ensure that the required deliverables are provided and meet acceptance criteria.

Recommendations:

We recommend that the Chief Financial Officer, in conjunction with the Assistant Secretary for Management and Chief Information Officer, take actions to:

2.1 Review the current PWS and ensure that sufficient documentation is required to support C&A recommendations and decisions.

2.2 Ensure that all future performance work statements for C&A contracts include requirements for documentation supporting scans, tests, and analyses conducted, and decisions made on the risks and mitigating factors considered, in support of the contractor's C&A recommendations.

Department Response

The Department did not concur with this finding, but concurred with both recommendations.

OIG Comments

See Attachment 3 for detailed comments to the Department's response.

OTHER MATTERS

During our audit, as discussed in Finding 1, the Department stated that a verbal agreement with the contractor was made regarding the definition of a vulnerability scan/penetration test finding. The Department further stated that the vulnerability scans and penetration tests conducted as part of the C&A review for the 10 Tier 4 systems did not result in any findings, so deliverables such as testing reports were not required. However, no evidence was available to support these statements, or the contractor's determination that the scans resulted in no findings. Department staff stated, and the contractor confirmed, that the analyses of scan results had been destroyed and were not available for review. As discussed in Finding 2, the PWS did not require the contractor to provide or maintain documentation supporting its conclusions and recommendations.

Throughout the review, OIG experienced delays in obtaining information from Department staff. OCIO staff had difficulty locating deliverables, and/or determining what documents, if any, the contractor provided to satisfy deliverable requirements. OCIO files were not complete and did not include evidence of inspection and acceptance or rejection of deliverables. Some deliverables that the Department stated were provided could not be located. Specifically, the following deliverables were not provided or could not be located – testing agreements, evidence that testing was conducted, test reports, certification recommendation report, and minutes of system owner and certifier out briefs. OCIO staff reported that a number of verbal agreements were made with the contractor regarding the scope of work, but no documentation existed to support any of these agreements.

In response to our draft report, the Department initially provided a response on October 4, 2004. The Department retracted that response on October 7, 2004. An amended response was provided on October 12, 2004. The Department retracted that response on October 14, 2004. The final response was provided on October 18, 2004. Some information in the response conflicted with information provided to us by Department officials during our review.

The conflicting information and multiple responses to the draft report received from the Department, along with our difficulties in obtaining information, indicate a lack of familiarity with contract requirements and with work actually accomplished. This supports our conclusion that the Department did not effectively manage the contract. It also lessens the Department's credibility with regard to any statements provided by Department management and staff during our review, especially in the absence of supporting documentation. As a result, we were presented with a scope limitation, in that we were unable to determine whether the vulnerability scans performed as part of the C&A effort resulted in any findings that should have been reported to management. As such, we were not able to determine whether some related deliverables should have been provided.

OBJECTIVE, SCOPE, AND METHODOLOGY

The objective of our audit was to determine the effectiveness of the Department's management of the C&A contract. Our audit was limited to review of deliverables related to the documentation review and vulnerability scans/penetration testing sections of the contract for the initial 10 Tier 4 systems subjected to the C&A process. Our audit evaluated activity under the C&A contract for these systems during the period June 25, 2003, through December 31, 2003. See Attachment 1 for further information on Tier 4 systems and the 10 systems included in our review.

To accomplish our objective, we obtained an understanding of the requirements for the C&A process, and for contract management and monitoring. We reviewed applicable laws and regulations, guidance on the C&A process provided by NIST and Departmental polices and procedures. We conducted interviews with OCIO and OCFO staff responsible for managing the C&A process and contract. We also interviewed staff from the C&A contractor. We obtained and reviewed documentation from OCIO and OCFO hard copy contract files, electronic files maintained by OCIO, and documentation from the C&A contractor.

To perform our audit, we reviewed the contract requirements for all deliverables related to the documentation review and vulnerability scans/penetration testing sections of the original contract. We obtained and reviewed documents submitted for those deliverables to determine whether the documents met the acceptance criteria specified in the contract.

Use of computer-processed data for this assignment was limited to payments made to the contractor in the Department's Financial Management Services System (FMSS). We matched the FMSS payment data to hard copy invoices submitted by the contractor to determine whether amounts on the invoices were the amounts paid. We noted no discrepancies in this review. Based on this assessment, we concluded the data was sufficiently reliable to support the amount of payments made to the contractor.

The conflicting information and multiple responses received from the Department, along with difficulties experienced obtaining information, and lack of documentation, reflects negatively on the Department's credibility, and presented a scope limitation for our audit. We were unable to determine whether the vulnerability scans performed as part of the C&A effort resulted in any findings that should have been reported to management. As such, we were not able to conclude whether deliverables regarding vulnerability scanning and penetration testing should have been provided by the contractor. This scope limitation is discussed further in the OTHER MATTERS section of this report.

We performed our fieldwork at applicable Department of Education offices in Washington, DC, during the period April 2004 through August 2004. We held an exit conference with Department management on August 2, 2004. Our audit was performed in accordance with generally accepted government auditing standards appropriate to the scope of the review as described above.

STATEMENT ON INTERNAL CONTROL

As part of our review, we performed a limited assessment of internal control applicable to the Department's management of the C&A contract. Our review was limited to identification and review of laws, regulations, guidelines, and Department policies and procedures related to the C&A process and contract management. We compared these requirements to the actual process followed to manage the C&A contract.

Because of inherent limitations, the assessment made for the limited purpose described above would not necessarily disclose all material weaknesses in the internal control. However, our assessment disclosed significant internal control weaknesses that adversely affected the Department's ability to effectively manage the C&A contract. These weaknesses and their effects are fully discussed in the AUDIT RESULTS section of this report.

TIER 4 SYSTEMS

The PWS, Section 4.1, equates the Department's "tiers" of systems to the security classification levels (SCLs) in NIST Special Publication 800-37. The PWS states:

> SCL-1 is appropriate for systems that raise low levels of concern due to their inherent risks. The Department classifies these systems as Tier 1 or 2. SCL-2 is appropriate for systems that raise moderate levels of concern and are classified as Tier 3 systems here at the Department. SCL-3 is appropriate for systems that raise high levels of concern and are classified as Tier 4 systems.

The 10 Tier 4 systems specified in the contract were as follows:[6]

1. EDNet
2. Education Central Automated Processing System
3. Federal Student Aid's Financial Management System
4. Common Origination and Disbursement
5. Central Processing System
6. Direct Loan Consolidation System
7. Direct Loan Servicing System
8. National Student Loan Data System
9. Postsecondary Education Participants System
10. Virtual Data Center

Section 4.1 of the PWS also states, "The level of effort required to C&A a system varies depending on the criticality (tier classification) of the system." Tier 4 systems are considered the most critical or highest risk, requiring the most significant level of effort in the C&A process. Specifically, the PWS requires the most documentation from system owners and most validation activities by the contractor for Tier 4 systems.

[6] The Common Services for Borrowers system was added as an additional Tier 4 system through Modification 0003 to the contract. Our audit did not include review of the deliverables for this system.

DETAILED RESULTS BY DELIVERABLE

Documentation Review:

Section 4.1.1 of the PWS, entitled "C&A Documentation Review," requires the contractor to review security documentation for the systems to ensure they are complete, consistent, contain adequate security controls, and comply with Department, OMB, and other policy guidance. The PWS requires review of the following documentation for each system:

- Risk Assessment (RA)
- Systems Security Plan (SSP)
- Configuration Management Plan (CMP)
- Continuity of Support (COS) Plan (and Disaster Recovery Plans, if applicable), and
- ST&E Plan

Deliverable 4.1.1.2 requires the contractor to provide a document detailing findings from document reviews and staff interviews. Acceptance criteria for this document include that findings should be consistent with Department, NIST, or best practice standards, should clearly explain how risk levels for any findings were determined, and should include specific names of those interviewed and exact locations of sites visited.

A Matrix of Observations was provided as the deliverable for this section. The following issues were noted with the matrices provided:

- Matrices for 2 of the 10 systems did not include a section documenting the ST&E plan review as required.
- Matrices for five of the systems included a sixth section for vulnerability scans/penetration testing, but data was only included in this section for two of the five systems. Since all 10 systems were to receive vulnerability scans/penetration testing, it would seem that all 10 systems should have this section completed.
- Matrices were incomplete for six of the systems in that some entries in the Continuity of Support plan did not have a risk impact listed, or listed "Yes" as the risk without an indication of the level of risk.
- We also found that the matrices did not meet acceptance criteria as the reports did not clearly explain how risk levels were determined (criterion 2b), and findings did not include specific names of those interviewed or locations of site visits (criterion 2c).

We matched the medium and high-risk issues noted in the matrices to determine whether the items were also noted in the system owner out briefs, certification recommendation report, and certifier out briefs. Only two systems had medium or high-risk items noted and all these items were also reflected in the later documents reviewed.

However, we noted that some medium or high-risk issues were noted in the system owner out briefs, certification recommendation report, or certifier out briefs that were not noted in the matrices. For example, we noted that these documents for the Virtual Data Center included two medium risk issues regarding the configuration management plan that were not included in the matrix of observations for that system.

Vulnerability Scans/Penetration Testing:

Section 4.1.3 of the PWS states that vulnerability scans and penetration testing provide an assessment of a system's ability to withstand intentional attempts to compromise systems security controls by exploiting vulnerabilities. The PWS states that the contractor shall develop, plan, and conduct vulnerability scans and penetration testing on all Tier 4 systems.

- Rules of Engagement (4.1.3.1.1) – According to the PWS, this was to be a document detailing agreement between the system owners and the contractor for vulnerability scans/penetration testing. This requirement indicates that system-specific rules of engagement would be developed. The contractor provided a general rules of engagement document for vulnerability scans/penetration testing, and this document also indicated that system-specific documents, to include appropriate signatures, contact information, dates of the tests, and other information, would be developed. OCIO staff were not able to locate any of the agreements for the 10 systems reviewed.

  The general rules did not include the Department's agreement with the contractor that penetration testing would not be performed if there was any possibility of bringing down a system, nor did the general rules document include the definition of a finding as agreed upon with the contractor. Both of these agreements were significant to the scope of work to be performed under the contract, but the Department could provide no documentation of the agreements, nor was the information provided to the CO for evaluation of the impact on the scope of work and contract price. (See further discussion of this issue in Finding 1.)

- Develop and Conduct Tests (4.1.3.1.3) – The contractor did not provide evidence that tests were conducted. Acceptance criteria for this deliverable required the contractor to provide "non-damaging evidence that the test was performed." OCIO staff stated that the deliverables were email or verbal communication that the testing had been completed, but OCIO could not locate any emails. OCIO staff stated that there was never any question that the testing was completed. However, without evidence as required by the contract, there is no assurance that the testing done was complete and appropriate.

- Evaluate and Document Findings (4.1.3.1.4) – This task was to result in a document detailing test findings and results. There were no particular requirements for the format of the document, other than that it should be included as an appendix to the test report in the next task. OCIO staff stated that there were no findings and therefore there were no deliverables for this task.

- Prepare Test Report (4.1.3.1.5) – This deliverable is a report detailing the methodology, findings, etc., from the vulnerability scans and penetration testing. Eight specific acceptance criteria were provided for the reports. OCIO staff stated that the deliverables for this task were a white paper provided at the start of the C&A project which detailed the methodology to be used, and the certifier out briefs (included in a later task). At least two of the acceptance criteria under this task were not satisfied by the deliverables cited by OCIO. Neither included the specific Internet Protocol address of the systems tested (criterion 1e), or the tools used and the settings of the tools (criterion 1f).

- System Owner Out Briefs (4.1.4.1.1) – This deliverable includes briefing slides that detail major ST&E and penetration test (if applicable) methodology and findings. The out briefs were to all have the same format, be consistent, free of spelling errors, etc. The contract required that the system owner out briefs have the same format and contain all information that will enable the system owner to implement necessary corrections, changes, or resolutions. We found that the out briefs were incomplete as follows:

    - Only 3 of the 10 briefings included an overview of the vulnerability scans/penetration testing process, listing vulnerability scanning tools used. None of the briefings listed the tool settings as required by the acceptance criteria.
    - Only 2 of the 10 briefings included a page on vulnerability scans/penetration testing that stated whether there were or were not findings.

  Since the out briefs were not complete, the system owners did not have all the data needed to make decisions or take corrective actions.

- Conduct Brief and Record Minutes (4.1.4.1.3) – No minutes were recorded as required. Neither the contractor nor OCIO staff were aware of this requirement. As such, there is no record of the discussion, or of the agreements for corrective action to be taken.

- Assurance that 2002 Risk Assessment Findings Have Been Mitigated (4.1.5) – While the certifier out briefs included a page on risk assessments that stated "no issues noted," there was no information to support this conclusion. No data was provided on what the former risk assessments were, or how they were mitigated. The matrices of observation stated only that the 2002 Risk Assessment Reports documented recommendations to mitigate the vulnerabilities, not that the vulnerabilities had actually been mitigated. As a result, the Department cannot evaluate the appropriateness of the contractor's conclusions and has no assurance that the risk assessment findings have been mitigated.

- Certification Recommendation Reports (4.1.5.1.2) – The contract includes a deliverable that details the system description, methodology, findings, recommendations, etc., and was to follow the basic format of a Risk Assessment Report included as an Appendix to a Department Directive. OCIO staff stated that after the first system manager's briefing, the COR verbally instructed the contractor that this report was not required as long as the methodology and specific findings were included in the certifier briefing. No documentation of this instruction was provided, nor was the CO informed of this change in requirements and elimination of this deliverable.

Further, we reviewed the requirements for the report and the certifier out briefs and found several sections in the report were not covered in the certifier out briefs or other deliverables, including the following – background, scope, structure, risk assessment approach (system boundaries, information-gathering techniques, steps taken to complete the risk assessment sections), system characterization, findings (existing mitigating security controls, impact analysis discussion sections), and appendices (system diagram, anticipated major changes/upgrades, glossary of terms, list of references, list of acronyms, list of key staff members and contact information).

This deliverable would have provided detail on how the C&A process was completed. By eliminating this requirement, OCIO reduced the amount of information to be provided by the contractor, and therefore reduced its assurance that the C&A process was appropriately performed.

- Certifier Briefing Slides (4.1.5.1.3) – Similar to the system owner out briefs, we found that that the certifier out briefs were not complete. Only 1 of the 10 briefings included information on the vulnerability scans/penetration testing results or that no vulnerabilities were found. As such, the certifier did not have complete information upon which to base the certification decision.

- Present executive brief, report, and letter to certifier, and record minutes, agreements, etc. (4.1.5.2.2) – No minutes were recorded as required. As with the systems owner briefs, neither the contractor nor OCIO staff were aware of this requirement.

OIG Comments to Department Response

In this attachment, the Department's response is presented in italics. OIG's comments to the Department's response are presented in standard type. The Department's entire response is provided as Attachment 4.

Department Response

TO: *Helen Lew*
Assistant Inspector General for Audit Services
Office of the Inspector General

FROM: *Jack Martin*
Chief Financial Officer
Office of the Chief Financial Officer

William Leidinger
Assistant Secretary for Management and the Chief Information Officer
Office of Management

SUBJECT: *Draft Audit Report Management of the Department's Certification and Accreditation Contract, Control Number ED-OIG/S19-E0015*

This memorandum responds to the Office of the Inspector General (OIG) subject Draft Audit Report, dated August 19, 2004. The purpose of the audit was to determine the effectiveness of the Department's management of the Certification and Accreditation (C&A) contract. The audit was limited to the review of deliverables related to the documentation review and vulnerability scanning/penetration testing requirement of the contract to the initial 10 Tier 4 systems subjected to the C&A process.

In general, the OIG found that the Department staff did not effectively manage the C&A contract and that improvements are needed in the Department's contract management process. The OIG reported that Department staff did not adequately track and inspect deliverables, gave unauthorized instructions to the contractor to reduce the scope of work to be performed, did not inform the contracting officer of changes in key personnel, and did not document evaluations of contractor-submitted reports. The OIG also reported that the performance work statement for the C&A contract did not require sufficient documentation to support C&A recommendations and decisions and that the initial services received from the C&A contractor did not provide

managers with complete, supportable information upon which to base their certification decisions.

Background

The Department had never before in its history completed the C&A of any IT system prior to the passage of the Government Information Security Reform Act in 2000. The Department began developing its C&A program in 2001 with its first Plan of Action and Milestones (POA&M) submission to the Office of Management and Budget (OMB). Department production systems began preparing for National Institute of Standards and Technology (NIST) compliant Risk Assessments that were completed the summer of 2002. The resulting risk assessment findings were incorporated into the Department's fiscal year 2002 POA&M. Systems across the Department applied the risk mitigation strategies described in NIST SP 800-30 while the Department further developed the C&A program.

The Department next launched an intensive effort to ensure that all Major Applications and General Support Systems had a NIST compliant System Security Plan, Configuration Management Plan and Contingency Plan (including a Disaster Recovery Plan for tier 3 and 4 systems). The Department also focused on developing standardized Security Test and Evaluation (ST&E) plans based on NIST and Department policies, standards and guidelines for consistent testing of all Tier 3 and 4 systems. The resulting ST&E plans were intended to verify that appropriate security controls existed and were functioning properly. The ST&E plans were never intended to identify system vulnerabilities, but rather vulnerabilities or weaknesses in security controls. Automated vulnerability scanning does not test the effectiveness of security controls, but instead identifies "potential" vulnerabilities in system configurations or software without taking into account the mitigating security controls in place. This approach for ST&E plans is supported by NIST Special Publication (SP) 800-37 Subtask 4.3, Security Assessment that states:

> *SECURITY ASSESSMENT*
> *SUBTASK 4.3: Assess the management, operational, and technical security controls in the information system using methods and procedures selected or developed.*
> *RESPONSIBILITY: Certification Agent.*
> *GUIDANCE: Security assessment determines the extent to which the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. The results of the security assessment, including recommendations for correcting any deficiencies in the security controls, are documented in the security assessment report.*

Each security control element that was to be tested had a test title, impact statement if the system control failed that particular test, test script with step-by-step instructions for executing the test, and expected results if the system control passed the test. This approach conformed to security industry standards for an ST&E plan.

The Department further consulted with several consulting firms experienced with supporting C&A programs for both civilian and Department of Defense agencies. The Department visited several civilian agencies with established C&A programs to learn from their successes and past experiences. The Department then wrote a Performance Work Statement (PWS) in order to contract for an independent, experienced IT security review team.

The resulting C&A PWS was shared with the OIG IT security auditors. The Department asked for assistance in ensuring that the C&A review described in the PWS would be adequate and meet Federal standards. The Department asked the OIG to assist in developing IT security standards that Agency systems should meet and against which these systems would be reviewed in the C&A program. In both instances, the OIG indicated that both of these activities were ED management responsibilities. The OIG did, however, provide checklists consisting of over 1000 questions used in their annual FISMA reviews. The checklists, however, did not include any associated risk levels with these questions or indicate the impact of mitigating controls. The OIG also provided a list of the automated vulnerability scanning tools that they use in their annual FISMA reviews. The assistance provided by the OIG was very much welcomed and appreciated.

Realizing the importance to the Department and high visibility of the C&A effort, the Department made every effort to ensure that sufficient resources were dedicated to manage the C&A contract. The Office of the Chief Information Officer (OCIO) did not have all of the required contracting, C&A subject matter expertise and project management skills in a single staff member. The Chief Information Officer (CIO), therefore, assigned the most experienced Contracting Officer's Representative (COR) to this project, as well as the entire Information Assurance staff to serve as subject matter experts in support of the COR. No one in OCIO, at the time, was both certified as a project manager and had experience with projects of similar size and scope. The CIO, therefore, contracted for a certified project manager who did meet these qualifications. These individuals formed the team designated to oversee the execution of the C&A contract. This team established several working groups that included key system owner representatives. The CIO met weekly with the management team, key system owner representatives, and the C&A contractor to ensure the success of the C&A effort.

The C&A contractor utilized the same scanning tools used by OIG for the FY03 FISMA audit during the CRG's C&A reviews of Mission Critical systems. The contractor did not, however, evaluate the resulting scan tool "hits" to have the same importance or relevance, as did the OIG. The contractor used an approach as described in NIST SP 800-42 that states on pages 3-4:

> *However, vulnerability scanners have some significant weaknesses. Generally, they only identify surface vulnerabilities and are unable to address the overall risk level of a scanned network. Although the scan process itself is highly automated, vulnerability scanners can have a high false positive error rate (reporting vulnerabilities when none exist). This means an individual with expertise in networking and operating system security and in administration must interpret the results.*

The Department contracted for the IT security expertise provided by the C&A contractor. The Department asked the C&A contractor to interpret the results of the scans. The C&A contractor did not believe that the scan "hits" identified anything significant regarding the existence of proper functioning of the related system security controls.

The C&A PWS asked the contractor to provide a report of any findings resulting from the vulnerability scanning and penetration testing. A definition of finding was not included in the PWS. The C&A contractor asked the Government to provide a definition. The OCIO Information Assurance staff provided a definition based on the only other source of "findings" with which they were familiar, namely OIG audits. A finding in an OIG audit is something that needs to be brought to the attention of the senior management official and needs to be subsequently corrected. The C&A contractor did not, in their professional opinion, identify anything from the vulnerability scanning and penetration testing that met this definition.

OIG Comments

As discussed in Finding 2 and in the OTHER MATTERS section of this report, the contract did not require the contractor to provide or maintain documentation supporting its conclusions, and Department staff stated analyses of scan results were destroyed. As a result, the Department does not have any documentation to support the contractor's determination that the scan "hits" did not identify any significant issues. Should any questions arise during the certification decision, the contractor should have the information available to resolve such questions.

The Department states that it based its definition of a "finding" on its interpretation of what constitutes a finding in an OIG audit. However, an OIG audit includes documentation of tests performed, information reviewed and evaluated, and the results of those reviews and evaluations, regardless of whether there were issues that needed to be reported to management. Using the Department's analogy, it is reasonable to expect that the C&A contractor could provide similar documentation to support its conclusions. As discussed in the report, the Department did not document its definition of a finding, or the agreement with the contractor as to what constitutes a finding. As a result, the contractor may have interpreted the definition in a manner not consistent with the Department's intent. Since documentation does not exist for what was or was not determined to be a finding, the Department does not have any assurance that the contractor followed its guidance on the definition of a finding in analyzing and reporting scan results.

Section 4.1.3 of the PWS, "Vulnerability Scan and Penetration Testing," states that vulnerability scans and penetration testing provide assessments of a system's ability to withstand intentional attempts to compromise system security controls by exploiting vulnerabilities. Without documentation that the tests were performed, and the results of those tests, whether favorable or unfavorable, the Department has only the verbal assurances of a contractor, with whom the Department has no previous experience, on the system's ability to withstand attempts to compromise controls.

Department Response

The C&A PWS also asked the contractor to take minutes at all out briefings and to provide a final C&A review report similar to the report format used for the previous system risk assessments. The intent was to ensure that the review methodology was clearly explained and that resulting findings, including associated risk level and recommended corrective action, were provided. When the C&A contractor provided advanced copies of their C&A briefing report, the C&A project management team believed that these materials fully met the intent of the reporting format, as well as the intent of the requirement regarding the taking of minutes. The COR verbally changed these requirements and the work continued with these modifications. OCIO Information Assurance staff believed that this experienced COR was following all of the Department's contract procedures.

OIG Comments

During our review, neither the contractor nor OCIO staff were familiar with the requirement for minutes of the meetings. It does not seem reasonable, therefore, that the COR accepted the briefing report as meeting the deliverable requirements for the minutes. Neither the contractor nor OCIO staff mentioned a verbal change to eliminate the requirement for the minutes as is stated in the Department's response. If the requirement for the deliverable had been eliminated, there was no documentation of this decision, nor was the CO made aware of the change in contract requirements so that an evaluation of any impact on the contract price could be made.

In addition, OCIO management stated during our review that items that were missing from the system and certifier outbriefs were covered verbally during the briefings. Had minutes been taken, this information would have been captured. Documents prepared prior to a meeting cannot capture key discussion items that may arise during meetings.

OCIO staff did state that after the first system manager's briefing, the COR verbally instructed the contractor that the Certification Recommendation Report was not required as long as the methodology and specific findings were included in the certifier briefing. As detailed in the audit report, we found that numerous sections in the Certification Recommendation Report, including sections dealing with the methodology (risk assessment approach, system boundaries, information-gathering techniques, steps taken to complete the risk assessment sections), were not covered in the certifier out briefs or other deliverables. No documentation of this instruction was provided, nor was the CO informed of this change in requirements and elimination of this deliverable.

In Modification 0005 to the contract, the Department included requirements for a "Final Security Assessment Report." This report includes essentially the same acceptance criteria as were included for the Certification Recommendation Report discussed above that OCIO staff stated was determined not to be needed during the original contract performance. This new report requirement indicates that Department staff determined that this information was needed for the C&A process.

Department Response

The designated C&A contract COR left the Department in the fall of 2003 following the completion of the first round of C&A. A second OCIO COR was identified. All of the deliverables for the second and third rounds of C&A were of the same quality and type as had been accepted under the first round. Everyone believed that proper procedures had been followed. Everyone was satisfied with the content and quality of deliverables and believed that the Department was properly moving forward to C&A all its systems and meet OMB's timeline.

OIG Comments

The Department states that all of the deliverables for the second and third rounds of C&A were of the same quality and type as accepted under the first round. This indicates that problems noted in our review, which encompassed the first and second rounds of C&A, continue into the third round.

The Department states, "Everyone was satisfied with the content and quality of the deliverables. . .." However, there was no documentation of inspection and acceptance of the deliverables, and the CO was not informed that requirements for the deliverables had been changed. Modification 0005 included requirement to repeat work performed under the original contract, indicating there were indeed deficiencies with the original work performed.

Department Response

Comments on the Draft Audit

The Department acknowledges that it could have improved contract monitoring efforts by reminding the COR of his/her basic contract monitoring responsibilities and limitations, specifically that

- *CORs, when using other Department staff and contractor project management support to assist with contract monitoring, are ultimately accountable to the contracting officer for the responsibilities in contract monitoring, and*
- *CORs are not authorized to direct changes to the contract and that CORs must communicate with their contracting officers to form a cooperative working relationship so that when changes are needed to contract requirements, the contracting officer can authorize such changes provided they are in the Government's best interest.*

However, while acknowledging that contract related processes early in the C&A contract period could have been performed to more closely adhere to the Department's contract procedures and policies, the Department does not concur in whole, with the findings of the draft audit. The Department believes that the C&A contractor's performance met the objectives of the contract in

support of the C&A program. A response to specific points in the draft audit is provided in the following.

OIG Comments

The Department states above its belief that ". . .the C&A contractor's performance met the objectives of the contract in support of the C&A program." The PWS states, "The Department's primary goal is to meet the C&A schedule as described under the Scope section of this document." The Scope section states the Department's intent to certify and accredit 10 systems by September 30, 2003, and an additional 15 systems by December 31, 2003. The Department did certify and accredit the systems as specified in the scope. As such, the Department's statement is accurate that the C&A contractor's performance met the objectives of the contract – to meet the schedule. However, due to changes made by the Department, and ineffective contract monitoring, we found that the contractor did not provide all deliverables originally required under the contract, and some deliverables provided did not meet acceptance criteria. As a result, the Department did not have information to support the decisions made by the contractor during its review, and the contractor's certification recommendations to the Department. The Department paid for work that was not performed under the contract.

Department Response

Finding No. 1 – Department Staff Did Not Effectively Manage the C&A Contract.

The Department agrees that as defined by ACS OCFO:2-108, Contract Monitoring for Program Officials, it is the policy of the Department to monitor every contract to the extent appropriate to provide assurance that the contractor performs the work called for in the contract, and to develop a clear record of accountability for performance. Elements of importance to the Department when monitoring for contractor performance include: contractor performance outcomes and specifications, timeliness, quality, and cost control. The PWS for the C&A contract stated that the scope of the PWS covers the responsibilities and activities of Phase 3, Validation of the C&A process and that the C&A contractor shall perform technical certification activities on behalf of the Certifier, and that the Department's primary goal is to meet the C&A schedule described under the Scope section of this document.[7]

a. The COR, other OCIO staff, and the project management contractor, did not adequately track and inspect deliverables to ensure that contract requirements were met.

The Department specified process outputs, deliverables, acceptance criteria, and dates due. The OIG reports that deliverables were not provided.

[7] *PWS, Section 3 – Scope, and Section 4 - Task 4.1, "Certification Review Group Support".*

The Department disagrees with the following.

Rules of Engagement, Evidence that Vulnerability Scans/Penetration Testing was Conducted, Minutes for System Owner and Certifier Out Briefs. The COR accepted the single rules of engagement deliverable from the contractor as meeting this requirement for all of the systems. System managers required testing agreements that detailed when and how the tests would be conducted. These agreements were negotiated at meetings attended by C&A contract management team members. It is not possible to complete the scanning logistics at the VDC, Rockville, EDNet or COD without establishing these agreements. This is standard practice and common knowledge. The audit occurred four to six months after the end of the related contract period. Although OCIO has not been able to locate any copies of these agreements, it would not have been possible for ICS to execute the scans and ST&E tests without such agreements. The COR accepted the communications at the weekly working group meetings that confirmed non-damaging execution of the vulnerability scans and penetration testing as the related deliverable. The COR accepted the Microsoft PowerPoint report as meeting the deliverable requirements for the minutes.

OIG Comments

Rules of Engagement/Testing Agreements

The Department could not provide any documentation to support that the COR accepted the general rules of engagement document for all systems. The general rules of engagement stated that system-specific documents, to include appropriate signatures, contact information, dates of the tests, and other information, would be developed. This information was not included in the general rules document. Acceptance criteria for this deliverable also included system-specific rules.

During our review, OCIO staff stated in an email on July 28, 2004, "We had one Rules of Engagement and then separate testing agreements. We are looking for copies of the testing agreements." At the exit conference on August 2, 2004, OCIO staff stated that they could not locate any of the testing agreements. OCIO staff stated that they had asked for these documents from both the system owners and the contractor and no one could find the agreements for any of the 10 Tier 4 systems. In its response above, the Department stated that although no copies of the agreements had been found, it would not have been possible to execute the scans and ST&E tests without such agreements. It seems highly unlikely if such agreements were developed, as the Department states is "standard practice and common knowledge," that not one copy could be located for any of the 10 systems. Without documentation, the Department cannot conclude that the testing agreements were developed as required by the general rules statement. This, combined with a lack of evidence that testing was completed and a lack of testing reports as discussed below, results in the fact that there is no documentation of what testing was actually performed.

Evidence that Vulnerability Scans/Penetration Testing Was Conducted

As stated in the report, acceptance criteria for this deliverable required the contractor to provide "non-damaging evidence that the test was performed" (emphasis added). During our review, OCIO staff stated that the deliverables consisted of emails or verbal communications that the testing had been completed, but OCIO staff could not locate any emails. OCIO staff stated there was never any question that the testing was completed. However, without evidence as required by the contract, there is no assurance that the testing done was complete and appropriate.

Minutes for System Owner and Certifier Out Briefs

The Department stated, "The COR accepted the Microsoft PowerPoint report as meeting the deliverable requirements for the minutes."

The Department's response to the System Owner Out Briefs section below states, ". . .the Department acknowledges that some of the items were verbally reported by the CRG." The PWS under 4.1.4 states,

> The purpose of these out briefs is to inform the system owners of the certification review results and to document any specific action items and agreements that come out of the meetings.

Without minutes of the meetings, there is no documentation of who attended, of action items and agreements, or of the items that the Department states were verbally reported.

During our review, neither the contractor nor OCIO staff were familiar with the requirement for minutes of the meetings. It does not seem reasonable, therefore, that the COR accepted the PowerPoint report as meeting these deliverable requirements. Neither the contractor nor OCIO staff mentioned a verbal change to eliminate the requirement for the minutes as is stated in the Department's response. There was no documentation of such a decision, nor was the CO made aware of the change in contract requirements so that an evaluation of any impact on the contract price could be made.

Department Response

Matrices of Observations, Vulnerability Scans/Penetration Testing Reports, System Owner and Certifier Out Briefs. The matrices of observation were not a required deliverable. They were work papers that supported the required deliverable of analysis of the security documentation. The required analysis was provided in the out brief presentation. The contractor voluntarily provided the Matrices of Observations for most systems on the CDs that included contract required deliverables at the time of Certifier Out Briefings. The Matrices of Observations were not, however, deliverables required under the contract. After the initiation of the C&A contract

audit and OIG began to ask questions about the Matrices of Observations, OCIO included the matrices in the analysis of everything ICS provided to the Department. This analysis was tracked in an Excel Workbook. The Excel workbook was never used during the related contract period to track required deliverables. The COR required vulnerability scanning and penetration test reports for items that the contractor believed should be brought to the attention of the Certifier. Since there were no such items, there were no related deliverables. While the Department agrees that the briefing reports were not totally consistent, the out briefs did meet the deliverable requirements; although the Department acknowledges that some of the items were verbally reported by the CRG. The Department takes further exception to the OIG assertion that the deliverables did not meet the acceptance criteria. The COR judged the deliverables referenced in this sub-finding as meeting the acceptance criteria.

OIG Comments

Matrices of Observations

On May 25, 2004, OCIO provided by email an Excel file entitled "C&A Deliverable Analysis." In the accompanying message, OCIO staff stated, "Attached is a workbook that provides the current status of the quality review OCIO is completing on all of the ICS deliverables under the C&A contract." The matrices of observation were included in this worksheet as a deliverable being tracked by OCIO. In its response above, the Department stated that OCIO included the matrices in the analysis after the OIG began asking questions about them. However, OIG's review was initially limited to review of the vulnerability scans/penetration testing deliverables, not those from the documentation review portion of the contract. OIG did not ask about the matrices until July 2, 2004, as discussed further below. As such, the Department was tracking the matrices as a deliverable prior to OIG's inquiries.

In an email on July 2, 2004, from OIG to OCIO, OIG staff stated,

> . . .I'm looking for the Matrix of Observations (MOOs) for the following systems. . .I'm assuming that this is what was used to report out on the results of ICS's documentation review for each system. Please advise if I am incorrect here in assuming that the MOOs were the documentation review deliverables.

OCIO staff responded by providing the additional matrices requested by OIG. OCIO did not at that time clarify that the matrices did not represent the deliverables for the documentation review, or that the matrices were not deliverables at all. At the exit conference where the detailed information from the audit was presented, including the attachment to the draft audit report that reported issues for each deliverable area and identified the matrices as the deliverable for the documentation review, OCIO staff did not mention that the matrices were not the deliverables for this area. Further, if the Department now asserts that the matrices of observations were not the deliverables under this section, then no deliverables were provided for the Documentation Review.

Vulnerability Scans/Penetration Testing Reports

In its response, the Department stated,

> The COR required vulnerability scanning and penetration test reports for items that the contractor believed should be brought to the attention of the Certifier. Since there were no such items, there were no related deliverables.

During our review, OCIO staff stated that the deliverables for this task were a white paper provided at the start of the C&A project, which detailed the methodology to be used, and the certifier out briefs. However, as stated in the audit report, these documents did not meet all acceptance criteria required for the testing reports – specifically, these documents did not include the Internet Protocol address of the systems tested and the tools used and setting for the tools. Combined with the lack of testing agreements, lack of evidence that testing was completed as discussed above, and documentation supporting the contractor's analysis of scan results being destroyed, the Department cannot determine whether the tests performed were appropriate. In addition, it would seem reasonable that negative reports could have been prepared by the contractor to provide the Department with documented assurance that there were no issues noted that should be brought to the attention of management.

System Owner and Certifier Out Briefs

The Department acknowledged the out briefs were not consistent. The out briefs did not contain all information required by the contract, and the Department also stated that some items were reported verbally. As such, the out briefs clearly did not meet acceptance criteria and should not have been accepted by the COR. There was no documentation of acceptance of any deliverables by the Department. Since no minutes were kept of the out briefs, there was no documentation to support the Department's statement that some items were reported verbally and not included in the out brief slides.

Department Response

Assurance that 2002 Risk Assessment Findings Have Been Mitigated. The OIG further reports that the contractor did not report on whether issues noted in the 2002 risk assessments had been mitigated as required by the contract. The Department submits that no system entered the C&A process with open risk assessment findings. All system managers stated in writing, that all risk assessment findings had been corrected. The C&A contractor verbally confirmed that all risk assessment findings had been addressed. The COR accepted this verbal confirmation, in concert with the documentation provided by system managers, as meeting the deliverable requirement.

OIG Comments

The PWS required the contractor to ". . .provide assurance that all risk assessment findings that are categorized as high and medium have been mitigated. . .." In its response, the Department stated that the contractor provided and the COR accepted verbal confirmation that all risk assessment findings had been addressed. Without documentation, the Department cannot evaluate the appropriateness of the contractor's conclusions or determine what the contractor actually did to assure the findings were mitigated.

Department Response

Inconsistency Between Matrices of Observations and System Owner and Certifier Out Briefs.
Lastly, the OIG reports that issues reported in the matrices of observations were not consistent with issues reported in the system owner and certifier out briefs. As stated previously, the matrices of observations were not a deliverable under this contract. These documents reflect the initial review of the security documentation by the C&A contractor. It was an established and government approved process to allow the system manager to correct any findings during the review and thereby remove such findings from the resulting report. The C&A review was never intended to be an audit, but rather a report of the security posture of the system in question at the time of the Certifier briefing. All issues listed in the matrices of observations that were not in out briefs were validated as corrected prior to the out briefs.

OIG Comments

OIG acknowledges that items corrected during the process would not appear in subsequent documents. However, OIG reported that the subsequent documents reported issues that were not included in the matrices, an earlier document in the process. As such, the matrices were incomplete and did not report all issues. The inconsistency in the reports should have been noted and resolved to determine why the matrices did not include the issues that were noted in subsequent documents. The fact that complete and consistent products were not provided by the contractor may indicate issues with the quality of the work performed.

Department Response

a(1) Deliverables were not adequately tracked and inspected for 3 reasons.

OCIO Fragmented Contract Management Responsibilities

The Department agrees that per Department policy, the COR is responsible to the contracting officer for monitoring the programmatic or technical aspects of the contract. However, it is not uncommon, depending upon the size and complexity of a contract, for the program manager to allocate contract monitoring responsibilities for subcomponents of the contract to staff

possessing subject matter expertise and other staff with experience in contract monitoring to assist the COR in managing the technical requirements. The Department can, in some high -risk contract requirement situations, outsource project management responsibilities, provided these responsibilities are not inherently governmental. In order to protect the Department's IT assets as required under NIST and other guidelines, OCIO embarked on an effort to aggressively C&A its system. OCIO therefore, contracted for a certified and experienced project manager to help ensure that government staff established timelines and process consistency. While Department staff had subject matter expertise, none had sufficient project management certification or expertise with a project of this size and scope.

Monitoring Focused on Schedules, Not Deliverables

To reiterate, the Department's primary goal under this contract was to meet the C&A schedule described under the Scope section. The written audit trail of monitoring activities focused on the schedule because that was the most complex and varied element. However, the Department disagrees that deliverables were not also a focus of contract monitoring. The COR and staff reviewed actual deliverables which led to changes to requirements. While meeting the schedule may have been a primary focus, the quality of the review of the deliverables for acceptance was not sacrificed. Had the deliverables not met the acceptance criteria, the Department would not have considered the schedule met.

OIG Comments

The Department agreed that its primary goal was to meet the C&A schedule, but stated that the quality of the review of the deliverables for acceptance was not sacrificed. However, our review found that deliverables were not provided, or did not meet the acceptance criteria specified in the contract. Verbal changes were made to deliverable requirements that were not documented and further reduced the effort required by the contractor to document its work and support its conclusions. During our review, the second COR stated that she did not inspect the deliverables, but rather passed them to the project management contractor or other OCIO staff with technical expertise. We found that the COR and other OCIO staff were not familiar with some of the deliverable requirements, had difficulty locating deliverables, and could not initially tell us which systems received penetration testing. As such, we conclude that the quality of the review of the deliverables for acceptance was not sufficient to note problems and appropriately reject deliverables that did not meet contract requirements.

Department Response

Receipts Process for Service Contracts Does Not Document Acceptance of Deliverables

Payment under the contract was based on adequate progress in the form of six monthly progress payments and was not directly tied to the acceptance of deliverables. The Department believes that sufficient monthly progress was made by the contractor and was the basis for any payment.

It was not intended for the receipts process to be the source of documentation for accepting contract deliverables. However, should contract payment be based on deliverables, the receipts process is adequate for documenting the receipt and acceptance of deliverables. Furthermore, while the Department acknowledges that the audit trail for accepting deliverables is not present, the COR judged the deliverables received as meeting the acceptance criteria and therefore, performance incentive payments were properly made.

OIG Comments

As previously noted, the COR stated that she did not inspect the deliverables, but provided them to other OCIO staff with technical expertise. As such, the COR did not judge the deliverables received as meeting the acceptance criteria as stated by the Department above. Section B of the contract states, "The contractor will be paid the incentives above only if all deliverables for systems meet the acceptance criteria and due dates specified. . .." Our review found that while systems were certified by the due dates, some deliverables to support the certification decision were not provided or did not meet acceptance criteria. The Department had no basis for granting the incentive payments, since there was no documentation of inspection and acceptance of the deliverables.

Department Response

b. OCIO staff gave unauthorized instructions to the contractor to reduce the scope of work to be performed.

The Department agrees with the OIG finding that the COR was not authorized to direct changes to the contract and that the contracting officer was unaware that these clarifications and changes were made in the contract requirements. Additionally:

- *The Department concurs that a special arrangement was reached with TYSY [sic], the COD vendor, and their auditor, KPMG, to have the C&A contractor observe KPMG perform the vulnerability scans and penetration testing for the COD system as part of the TYSY [sic] SAS 70 audit. The scans that were conducted as part of the normal SAS 70 audit were deemed satisfactory by the C&A contractor for purposes of the C&A effort. The C&A contractor conducted their independent analysis of the scan results and based their required deliverable, the C&A analysis report, upon this process. The C&A contractor acknowledged that their November 5, 2003 Weekly Status Report misstated the issues surrounding the COD scanning. The COR staff and FSA staff believed that the C&A contractor met the vulnerability scanning deliverable requirements. Subsequent to this work, KPMG, in the normal course of their engagement with TYSY [sic], destroyed the scan results. This is KPMG's normal practice. Consistent with the rules of engagement summarized in the meeting minutes dated 9/11/2003, the KPMG work papers and other output and results could not be removed from the TSYS' premises. Consequently, evidence that the scans were executed, results produced and analyzed no*

longer exist or cannot be made available to ED under the rules of engagement. ED is in the process of obtaining security sign in/out documentation from TYSY [sic] and affidavits/attestations from the C&A contractor to attest to their presence on-site at TSYS when KPMG performed the SAS 70 scans.

OIG Comments

The SAS 70 audit was a regular audit performed by KPMG, and not tailored to the C&A review. As stated in the Department's response, the COD contractors did not install the vulnerability scanning tools or configure these tools according to the C&A contractor's specifications. The C&A contractor merely observed the vulnerability scans and penetration testing conducted as part of the normal SAS 70 audit.

OIG maintains its position that this reduced the level of effort by the contractor and OCIO should have discussed this with the CO to determine if a reduction in contract price was warranted.

Department Response

- *The Department concurs that the C&A contractor did not execute the vulnerability scans for DLSS. The DLSS contractors (ACS) runs routine scans of DLSS. A routine scan of DLSS was performed by ACS in October 2003. Please note that the C&A contractor was not present for and, therefore, did not observe the actual configuration of the software and execution of this routine scan. The C&A contractor did communicate with ACS about the software and types of scans that ACS performs on DLSS. Based on the information provided by ACS, the C&A contractor determined that the software used and scans performed by ACS were the same that they (the C&A contractors) used in the C&A process. The C&A contractors requested and used ACS's October 2003 scan results for their C&A analysis and based their required deliverable, the C&A analysis report upon this process. The COR staff and FSA staff believed that the C&A contractor met the vulnerability scanning deliverable requirement.*

OIG Comments

The Department concurred that the C&A contractor was not present to observe the vulnerability scans, but rather reviewed scans run by the DLSS contractor as part of its routine processes. OIG maintains its position that this reduced the level of effort by the contractor and OCIO should have discussed this with the CO to determine if a reduction in contract price was warranted.

Department Response

- *The Department does not agree with the OIG interpretation on the contract requirements for penetration testing. The contract specifically required penetration testing to leverage vulnerabilities discovered during the scans. Since no vulnerabilities that met the agreed upon definition of 'finding' were discovered, there was nothing to attempt to leverage via penetration testing.*

OIG Comments

During our review, we were informed that it was the Department's concern with interrupting system operations that resulted in penetration testing not being performed (except for COD by KPMG as part of its SAS 70 review), not a lack of issues noted in vulnerability scanning. In a letter to the OIG dated May 25, 2004, ICS stated:

> ICS identified and conveyed to the Office of the Chief Information Officer (OCIO) those systems where penetration testing was the preferred method. On September 9, 2003, the OCIO COR discussed with ICS the concern for disruption of systems as a result of penetration testing on mission-critical systems. . .As a result of several meetings with the OCIO, ICS agreed that penetration testing would not be performed on those systems where an impact to ongoing operations was anticipated.

In an email to OIG on June 18, 2004, ICS stated that one system was considered for full penetration testing. All other systems were considered too operationally valuable to risk bringing them down from any penetration testing. Since the contractor's accepted proposal included pricing for penetration testing, OCIO staff should have contacted the CO to discuss the reduction in the scope of work so that an appropriate reduction in the contract price could be evaluated.

Department Response

- *While the Department is in agreement that the COR did not perform all of his/her duties in conformance with Department policy, the Department is not convinced that the unauthorized changes and direction that occurred is as a result of a fragmented COR monitoring team. As stated previously, all CORs assigned to this contract each had a number of years experience as IT contract CORs.*

OIG Comments

While the Department does not believe the issues were due to a fragmented monitoring team, it did not offer another reason for the problems noted. Earlier in its response, (see page 3 of this attachment), the Department stated that it made every effort to ensure

sufficient resources were dedicated to manage the C&A contract. However, the second COR stated that she was not able to devote a great deal of time to this contract as she was also assigned other tasks. The monitoring team established did not effectively communicate. We found that despite the organizational structure put into place to monitor the C&A process, the COR and/or team did not:

- Adequately track and inspect deliverables,
- Ensure instructions provided to the contractor were appropriate,
- Document and involve the CO where appropriate,
- Ensure the CO was informed of key personnel changes, and
- Ensure evaluations of contractor-submitted reports were documented and provided to the CO.

As such, contract monitoring activities were fragmented and not appropriately coordinated with the COR and CO. The Department concurred with the recommendations made in this area.

Department Response

- *The Department concurs that verbal agreements with the contractor presented the possibility of future confusion and/or disagreements; however, these agreements did not result in a reduced level of effort that impacted price. The verbal agreements clarified the original intent of the contract and the level of effort for which we contracted was received.*

OIG Comments

OIG strongly disagrees with the Department's response. Verbal agreements resulted in elimination of deliverables (or substitution of the documents called for in the Performance Work Statement with verbal reports), or reduction in the work performed by the C&A contractor in the following areas:

- System Specific Rules of Engagement/Testing Agreements
- Evidence that tests were conducted
- Vulnerability Scanning at COD and DLSS
- Penetration testing for all 10 Tier 4 Systems
- Testing reports
- Minutes of System Owner and Certifier Outbriefs
- Certification Recommendation Reports

Elimination of the requirements for written documents reduced the level of effort by the contractor and a commensurate reduction in the price should have been negotiated. As stated in the report, the Department issued Modification 0005 to the contract to have the

contractor reperform some of the C&A tasks. This modification clearly indicates the tasks were not performed satisfactorily in the original contract term. This modification had a total cost of $715,851. For the 10 Tier 4 systems in our review, the value of the C&A tasks included in the modification was $253,692. Of this amount, $122,472 was to repeat C&A analyses for seven of the Tier 4 systems that should have been completed in the initial contract.

Department Response

- *The Department does not concur that the verbal agreements regarding the extent of penetration testing for the Tier 4 systems resulted in less assurance for the Department that these high-risk systems were adequately protected against unauthorized access. We believe most Federal civilian agencies do not utilize vulnerability scanning or penetration testing in their C&A reviews. The Department opted for a C&A review that exceeded that employed at the majority of Federal civilian agencies because we wanted to provide a higher level of assurance. We believe that that higher level of assurance was realized.*

OIG Comments

OIG's position is unchanged. The contract called for penetration testing of the 10 Tier 4 systems. The contract stated that vulnerability scans and penetration testing provide an assessment of a system's ability to withstand intentional attempts to compromise systems security controls by exploiting vulnerabilities. This task was not completed as required by the contract, as only 1 of 10 systems received penetration testing. The current modification to the contract requires penetration testing to be performed for all 10 systems, which would seem to contradict the Department's statement that a high level of assurance was previously realized.

Department Response

c. The COR/OCIO staff did not ensure that the CO was informed of changes in key personnel and that the contractor submitted to the CO formal notice and requests for written approval of substitution of key personnel.

The Department concurs with this finding. However, the Department disputes that the level of knowledge of the contractor personnel substituted without the knowledge of the contracting officer may not have equaled that of the designated key personnel upon which the contract award decision was at least partially based. Although the contracting officer was not properly involved with these personnel changes, the C&A project management team did closely review and discuss these changes prior to implementation. The resumes and qualifications were reviewed before personnel changes were made. The level of service and personnel skills and

expertise were specifically addressed and monitored. The Department did not receive any reduction in service or quality. For the OIG to infer this is purely speculative in nature.

OIG Comments

The Department concurred with this finding and related recommendation. The Department states that qualifications were reviewed before key personnel changes were made. However, the contract and COR files had no documentation of review of resumes or qualifications for substituted key personnel.

Department Response

d. The COR did not document evaluations of contractor-submitted reports or provide written evaluations of the reports to the CO.

The Department concurs with this finding. The C&A contractor delivered the reports; however, the Department acknowledges that the subsequent audit trail of reviews does not exist. The OIG purports that potential problem indicators included in the reports may not have been detected by the COR and in consideration that the contracting officer was not provided evaluations to confirm that reports were being received as required by the contract to take any required action to protect the Government's interest. The Department does not believe that any potential problems were overlooked.

OIG Comments

The Department concurred with the finding and recommendation.

Department Response

Department Response to OIG Recommendations for Finding No. 1

1.1.a The Department concurs with this recommendation. A customized database has been implemented to assist in tracking deliverables at the requirements level. Requirements checklists have been developed that are used to validate formal acceptance of all deliverables. Formal deliverable acceptance is documented in writing.

1.1.b The Department concurs with this recommendation. The contracting officer is specifically cited throughout the modified PWS as the only authorized individual to make any changes to the contract.

1.1.c The Department concurs with this recommendation. The contracting officer notification of key personnel changes is already in effect.

1.1.d The Department concurs with this recommendation. The COR has already begun documenting contractor reports and submitting the evaluations to the contracting officer.

1.1.e The Department concurs with this recommendation. The COR has already begun building a proper contract file that reflects all information required to carry out the monitoring responsibilities.

1.2 The Department concurs with this recommendation. Several meetings have already taken place beginning in July 2004, to discuss the contract monitoring plan and to clarify roles and responsibilities.

1.3 The Department concurs with this recommendation. Processes are already in place that ensures that any substitution in key personnel follow appropriate procedures.

1.4 The Department concurs with this recommendation. The contracting officer will ensure that any changes in COR responsibilities receive the proper appointment memoranda.

1.5 The Department does not concur with the underlying findings for this recommendation and therefore does not concur with the recommendation. The Department does not concur that incentive payments were made to the contractor improperly, that deliverables were unacceptable, or that payment was made for more than it should have for the work completed. The Contracting Officer had already determined that an opinion is not required from Office of General Counsel.

OIG Comments

The Department concurred with four of the five recommendations for this finding. The Department did not concur with OIG's Recommendation 1.5 to obtain an Office of General Counsel opinion regarding possible remedies to recover funds from the contractor for improper incentive payments, unacceptable deliverables, and reductions to the scope of work made without the authorization of the CO.

As discussed in Finding 1, contract terms stated that incentives would be paid only if all deliverables meet the acceptance criteria and due dates specified. Since not all deliverables were provided, and some deliverables were not complete and therefore did not meet acceptance critieria, the contractor should not have been paid any of the incentive amounts. OIG continues to recommend that OGC be consulted for an opinion on this matter.

Department Response

Finding No. 2 - The Performance Work Statement Did Not Require Sufficient Documentation to Support C&A Recommendations and Decisions

The Department does not agree that the original PWS did not require sufficient documentation to support certification decisions. The documentation requirements in the original PWS were consistent with those in other Federal agencies and based on Federal guidelines to support C&A recommendations and decisions. NIST 800-34 places the emphasis on the System Security Plan and the Security Test and Evaluation (ST&E) plan. The original PWS placed a similar emphasis on these two areas as the basis for the subsequent C&A recommendations and decisions. Thorough and consistent ST&E plans were executed for each of the 10 systems reviewed in this audit.

Department Response to OIG Recommendations for Finding No. 2

2.1. The Department concurs with this recommendation and this action is completed.

2.2. The Department concurs with this recommendation. This action has been implemented with the current contract modification that will be a template for future C&A contracts.

Thank you again for this opportunity to respond. Should you have questions, please contact Glenn Perry, Director, Contracts and Acquisitions Management at (202) 245-6200.

OIG Comments

The Department stated that it disagreed with this finding, but concurred with both of the related recommendations. The Department stated that actions to address Recommendation 2.2 -- to include requirements for documentation supporting scans, tests, and analyses conducted, and decisions made on the risks and mitigating factors considered, in support of the contractor's C&A recommendations -- were implemented with the current modification to the C&A contract.

In its response, the Department states that NIST 800-34 places the emphasis on the System Security Plan and the ST&E plan. While review of the ST&E deliverables was not a part of this audit, analysis of these deliverables was conducted as part of the OIG's Federal Information Security Management Act (FISMA) audit. OIG disagrees with the Department's statement that "Thorough and consistent ST&E plans were executed for each of the 10 systems reviewed in this audit." In its FISMA audit, OIG determined that ST&E procedures were not sufficient to adequately identify residual system security risks and to ensure that significant security weaknesses identified in prior OIG security evaluations were fully corrected.

Department Response to Draft Report
October 18, 2004

TO: Helen Lew
Assistant Inspector General for Audit Services
Office of the Inspector General

FROM: Jack Martin
Chief Financial Officer
Office of the Chief Financial Officer

William Leidinger
Assistant Secretary for Management and the Chief Information Officer
Office of Management

SUBJECT: Draft Audit Report *Management of the Department's Certification and Accreditation Contract*, Control Number ED-OIG/S19-E0015

This memorandum responds to the Office of the Inspector General (OIG) subject Draft Audit Report, dated August 19, 2004. The purpose of the audit was to determine the effectiveness of the Department's management of the Certification and Accreditation (C&A) contract. The audit was limited to the review of deliverables related to the documentation review and vulnerability scanning/penetration testing requirement of the contract to the initial 10 Tier 4 systems subjected to the C&A process.

In general, the OIG found that the Department staff did not effectively manage the C&A contract and that improvements are needed in the Department's contract management process. The OIG reported that Department staff did not adequately track and inspect deliverables, gave unauthorized instructions to the contractor to reduce the scope of work to be performed, did not inform the contracting officer of changes in key personnel, and did not document evaluations of contractor-submitted reports. The OIG also reported that the performance work statement for the C&A contract did not require sufficient documentation to support C&A recommendations and decisions and that the initial services received from the C&A contractor did not provide managers with complete, supportable information upon which to base their certification decisions.

Background

The Department had never before in its history completed the C&A of any IT system prior to the passage of the Government Information Security Reform Act in 2000. The Department began developing its C&A program in 2001 with its first Plan of Action and Milestones (POA&M)

submission to the Office of Management and Budget (OMB). Department production systems began preparing for National Institute of Standards and Technology (NIST) compliant Risk Assessments that were completed the summer of 2002. The resulting risk assessment findings were incorporated into the Department's fiscal year 2002 POA&M. Systems across the Department applied the risk mitigation strategies described in NIST SP 800-30 while the Department further developed the C&A program.

The Department next launched an intensive effort to ensure that all Major Applications and General Support Systems had a NIST compliant System Security Plan, Configuration Management Plan and Contingency Plan (including a Disaster Recovery Plan for tier 3 and 4 systems). The Department also focused on developing standardized Security Test and Evaluation (ST&E) plans based on NIST and Department policies, standards and guidelines for consistent testing of all Tier 3 and 4 systems. The resulting ST&E plans were intended to verify that appropriate security controls existed and were functioning properly. The ST&E plans were never intended to identify system vulnerabilities, but rather vulnerabilities or weaknesses in security controls. Automated vulnerability scanning does not test the effectiveness of security controls, but instead identifies "potential" vulnerabilities in system configurations or software without taking into account the mitigating security controls in place. This approach for ST&E plans is supported by NIST Special Publication (SP) 800-37 Subtask 4.3, Security Assessment that states:

> SECURITY ASSESSMENT
> SUBTASK 4.3: Assess the management, operational, and technical security controls in the information system using methods and procedures selected or developed.
> RESPONSIBILITY: Certification Agent.
> GUIDANCE: Security assessment determines the extent to which the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. The results of the security assessment, including recommendations for correcting any deficiencies in the security controls, are documented in the security assessment report.

Each security control element that was to be tested had a test title, impact statement if the system control failed that particular test, test script with step-by-step instructions for executing the test, and expected results if the system control passed the test. This approach conformed to security industry standards for an ST&E plan.

The Department further consulted with several consulting firms experienced with supporting C&A programs for both civilian and Department of Defense agencies. The Department visited several civilian agencies with established C&A programs to learn from their successes and past experiences. The Department then wrote a Performance Work Statement (PWS) in order to contract for an independent, experienced IT security review team.

The resulting C&A PWS was shared with the OIG IT security auditors. The Department asked for assistance in ensuring that the C&A review described in the PWS would be adequate and meet Federal standards. The Department asked the OIG to assist in developing IT security standards that Agency systems should meet and against which these systems would be reviewed

in the C&A program. In both instances, the OIG indicated that both of these activities were ED management responsibilities. The OIG did, however, provide checklists consisting of over 1000 questions used in their annual FISMA reviews. The checklists, however, did not include any associated risk levels with these questions or indicate the impact of mitigating controls. The OIG also provided a list of the automated vulnerability scanning tools that they use in their annual FISMA reviews. The assistance provided by the OIG was very much welcomed and appreciated.

Realizing the importance to the Department and high visibility of the C&A effort, the Department made every effort to ensure that sufficient resources were dedicated to manage the C&A contract. The Office of the Chief Information Officer (OCIO) did not have all of the required contracting, C&A subject matter expertise and project management skills in a single staff member. The Chief Information Officer (CIO), therefore, assigned the most experienced Contracting Officer's Representative (COR) to this project, as well as the entire Information Assurance staff to serve as subject matter experts in support of the COR. No one in OCIO, at the time, was both certified as a project manager and had experience with projects of similar size and scope. The CIO, therefore, contracted for a certified project manager who did meet these qualifications. These individuals formed the team designated to oversee the execution of the C&A contract. This team established several working groups that included key system owner representatives. The CIO met weekly with the management team, key system owner representatives, and the C&A contractor to ensure the success of the C&A effort.

The C&A contractor utilized the same scanning tools used by OIG for the FY03 FISMA audit during the CRG's C&A reviews of Mission Critical systems. The contractor did not, however, evaluate the resulting scan tool "hits" to have the same importance or relevance, as did the OIG. The contractor used an approach as described in NIST SP 800-42 that states on pages 3-4:

> However, vulnerability scanners have some significant weaknesses. Generally, they only identify surface vulnerabilities and are unable to address the overall risk level of a scanned network. Although the scan process itself is highly automated, vulnerability scanners can have a high false positive error rate (reporting vulnerabilities when none exist). This means an individual with expertise in networking and operating system security and in administration must interpret the results.

The Department contracted for the IT security expertise provided by the C&A contractor. The Department asked the C&A contractor to interpret the results of the scans. The C&A contractor did not believe that the scan "hits" identified anything significant regarding the existence of proper functioning of the related system security controls.

The C&A PWS asked the contractor to provide a report of any findings resulting from the vulnerability scanning and penetration testing. A definition of finding was not included in the PWS. The C&A contractor asked the Government to provide a definition. The OCIO Information Assurance staff provided a definition based on the only other source of "findings" with which they were familiar, namely OIG audits. A finding in an OIG audit is something that needs to be brought to the attention of the senior management official and needs to be subsequently corrected. The C&A contractor did not, in their professional opinion, identify anything from the vulnerability scanning and penetration testing that met this definition.

The C&A PWS also asked the contractor to take minutes at all out briefings and to provide a final C&A review report similar to the report format used for the previous system risk assessments. The intent was to ensure that the review methodology was clearly explained and that resulting findings, including associated risk level and recommended corrective action, were provided. When the C&A contractor provided advanced copies of their C&A briefing report, the C&A project management team believed that these materials fully met the intent of the reporting format, as well as the intent of the requirement regarding the taking of minutes. The COR verbally changed these requirements and the work continued with these modifications. OCIO Information Assurance staff believed that this experienced COR was following all of the Department's contract procedures.

The designated C&A contract COR left the Department in the fall of 2003 following the completion of the first round of C&A. A second OCIO COR was identified. All of the deliverables for the second and third rounds of C&A were of the same quality and type as had been accepted under the first round. Everyone believed that proper procedures had been followed. Everyone was satisfied with the content and quality of deliverables and believed that the Department was properly moving forward to C&A all its systems and meet OMB's timeline.

Comments on the Draft Audit

The Department acknowledges that it could have improved contract monitoring efforts by reminding the COR of his/her basic contract monitoring responsibilities and limitations, specifically that

- CORs, when using other Department staff and contractor project management support to assist with contract monitoring, are ultimately accountable to the contracting officer for the responsibilities in contract monitoring, and
- CORs are not authorized to direct changes to the contract and that CORs must communicate with their contracting officers to form a cooperative working relationship so that when changes are needed to contract requirements, the contracting officer can authorize such changes provided they are in the Government's best interest.

However, while acknowledging that contract related processes early in the C&A contract period could have been performed to more closely adhere to the Department's contract procedures and policies, the Department does not concur in whole, with the findings of the draft audit. The Department believes that the C&A contractor's performance met the objectives of the contract in support of the C&A program. A response to specific points in the draft audit is provided in the following.

Finding No. 1 – Department Staff Did Not Effectively Manage the C&A Contract.

The Department agrees that as defined by ACS OCFO:2-108, Contract Monitoring for Program Officials, it is the policy of the Department to monitor every contract to the extent appropriate to provide assurance that the contractor performs the work called for in the contract, and to develop

a clear record of accountability for performance. Elements of importance to the Department when monitoring for contractor performance include: contractor performance outcomes and specifications, timeliness, quality, and cost control. The PWS for the C&A contract stated that the scope of the PWS covers the responsibilities and activities of Phase 3, Validation of the C&A process and that the C&A contractor shall perform technical certification activities on behalf of the Certifier, and that the Department's primary goal is to meet the C&A schedule described under the Scope section of this document.[8]

a. The COR, other OCIO staff, and the project management contractor, did not adequately track and inspect deliverables to ensure that contract requirements were met.

The Department specified process outputs, deliverables, acceptance criteria, and dates due. The OIG reports that deliverables were not provided.

The Department disagrees with the following.

Rules of Engagement, Evidence that Vulnerability Scans/Penetration Testing was Conducted, Minutes for System Owner and Certifier Out Briefs. The COR accepted the single rules of engagement deliverable from the contractor as meeting this requirement for all of the systems. System managers required testing agreements that detailed when and how the tests would be conducted. These agreements were negotiated at meetings attended by C&A contract management team members. It is not possible to complete the scanning logistics at the VDC, Rockville, EDNet or COD without establishing these agreements. This is standard practice and common knowledge. The audit occurred four to six months after the end of the related contract period. Although OCIO has not been able to locate any copies of these agreements, it would not have been possible for ICS to execute the scans and ST&E tests without such agreements. The COR accepted the communications at the weekly working group meetings that confirmed non-damaging execution of the vulnerability scans and penetration testing as the related deliverable. The COR accepted the Microsoft PowerPoint report as meeting the deliverable requirements for the minutes.

Matrices of Observations, Vulnerability Scans/Penetration Testing Reports, System Owner and Certifier Out Briefs.. The matrices of observation were not a required deliverable. They were work papers that supported the required deliverable of analysis of the security documentation. The required analysis was provided in the out brief presentation. The contractor voluntarily provided the Matrices of Observations for most systems on the CDs that included contract required deliverables at the time of Certifier Out Briefings. The Matrices of Observations were not, however, deliverables required under the contract. After the initiation of the C&A contract audit and OIG began to ask questions about the Matrices of Observations, OCIO included the matrices in the analysis of everything ICS provided to the Department. This analysis was tracked in an Excel Workbook. The Excel workbook was never used during the related contract period to track required deliverables. The COR required vulnerability scanning and penetration test reports for items that the contractor believed should be brought to the attention of the Certifier. Since there were no such items, there were no related deliverables. While the

[8] PWS, Section 3 – Scope, and Section 4- Task 4.1, "Certification Review Group Support".

Department agrees that the briefing reports were not totally consistent, the out briefs did meet the deliverable requirements; although the Department acknowledges that some of the items were verbally reported by the CRG. The Department takes further exception to the OIG assertion that the deliverables did not meet the acceptance criteria. The COR judged the deliverables referenced in this sub-finding as meeting the acceptance criteria.

Assurance that 2002 Risk Assessment Findings Have Been Mitigated. The OIG further reports that the contractor did not report on whether issues noted in the 2002 risk assessments had been mitigated as required by the contract. The Department submits that no system entered the C&A process with open risk assessment findings. All system managers stated in writing, that all risk assessment findings had been corrected. The C&A contractor verbally confirmed that all risk assessment findings had been addressed. The COR accepted this verbal confirmation, in concert with the documentation provided by system managers, as meeting the deliverable requirement.

Inconsistency Between Matrices of Observations and System Owner and Certifier Out Briefs. Lastly, the OIG reports that issues reported in the matrices of observations were not consistent with issues reported in the system owner and certifier out briefs. As stated previously, the matrices of observations were not a deliverable under this contract. These documents reflect the initial review of the security documentation by the C&A contractor. It was an established and government approved process to allow the system manager to correct any findings during the review and thereby remove such findings from the resulting report. The C&A review was never intended to be an audit, but rather a report of the security posture of the system in question at the time of the Certifier briefing. All issues listed in the matrices of observations that were not in out briefs were validated as corrected prior to the out briefs.

a(1) Deliverables were not adequately tracked and inspected for 3 reasons.

OCIO Fragmented Contract Management Responsibilities

The Department agrees that per Department policy, the COR is responsible to the contracting officer for monitoring the programmatic or technical aspects of the contract. However, it is not uncommon, depending upon the size and complexity of a contract, for the program manager to allocate contract monitoring responsibilities for subcomponents of the contract to staff possessing subject matter expertise and other staff with experience in contract monitoring to assist the COR in managing the technical requirements. The Department can, in some high-risk contract requirement situations, outsource project management responsibilities, provided these responsibilities are not inherently governmental. In order to protect the Department's IT assets as required under NIST and other guidelines, OCIO embarked on an effort to aggressively C&A its system. OCIO therefore, contracted for a certified and experienced project manager to help ensure that government staff established timelines and process consistency. While Department staff had subject matter expertise, none had sufficient project management certification or expertise with a project of this size and scope.

Monitoring Focused on Schedules, Not Deliverables

To reiterate, the Department's primary goal under this contract was to meet the C&A schedule described under the Scope section. The written audit trail of monitoring activities focused on the schedule because that was the most complex and varied element. However, the Department disagrees that deliverables were not also a focus of contract monitoring. The COR and staff reviewed actual deliverables which led to changes to requirements. While meeting the schedule may have been a primary focus, the quality of the review of the deliverables for acceptance was not sacrificed. Had the deliverables not met the acceptance criteria, the Department would not have considered the schedule met.

Receipts Process for Service Contracts Does Not Document Acceptance of Deliverables

Payment under the contract was based on adequate progress in the form of six monthly progress payments and was not directly tied to the acceptance of deliverables. The Department believes that sufficient monthly progress was made by the contractor and was the basis for any payment. It was not intended for the receipts process to be the source of documentation for accepting contract deliverables. However, should contract payment be based on deliverables, the receipts process is adequate for documenting the receipt and acceptance of deliverables. Furthermore, while the Department acknowledges that the audit trail for accepting deliverables is not present, the COR judged the deliverables received as meeting the acceptance criteria and therefore, performance incentive payments were properly made.

b. OCIO staff gave unauthorized instructions to the contractor to reduce the scope of work to be performed.

The Department agrees with the OIG finding that the COR was not authorized to direct changes to the contract and that the contracting officer was unaware that these clarifications and changes were made in the contract requirements. Additionally:

- The Department concurs that a special arrangement was reached with TYSY, the COD vendor, and their auditor, KPMG, to have the C&A contractor observe KPMG perform the vulnerability scans and penetration testing for the COD system as part of the TYSY SAS 70 audit. The scans that were conducted as part of the normal SAS 70 audit were deemed satisfactory by the C&A contractor for purposes of the C&A effort. The C&A contractor conducted their independent analysis of the scan results and based their required deliverable, the C&A analysis report, upon this process. The C&A contractor acknowledged that their November 5, 2003 Weekly Status Report misstated the issues surrounding the COD scanning. The COR staff and FSA staff believed that the C&A contractor met the vulnerability scanning deliverable requirements. Subsequent to this work, KPMG, in the normal course of their engagement with TYSY, destroyed the scan results. This is KPMG's normal practice. Consistent with the rules of engagement summarized in the meeting minutes dated 9/11/2003, the KPMG work papers and other output and results could not be removed from the TSYS' premises. Consequently, evidence that the scans were executed, results produced and analyzed no longer exist or cannot be made available to ED under the

rules of engagement. ED is in the process of obtaining security sign in/out documentation from TYSY and affidavits/attestations from the C&A contractor to attest to their presence on-site at TSYS when KPMG performed the SAS 70 scans.

- The Department concurs that the C&A contractor did not execute the vulnerability scans for DLSS. The DLSS contractors (ACS) runs routine scans of DLSS. A routine scan of DLSS was performed by ACS in October 2003. Please note that the C&A contractor was not present for and, therefore, did not observe the actual configuration of the software and execution of this routine scan. The C&A contractor did communicate with ACS about the software and types of scans that ACS performs on DLSS. Based on the information provided by ACS, the C&A contractor determined that the software used and scans performed by ACS were the same that they (the C&A contractors) used in the C&A process. The C&A contractors requested and used ACS's October 2003 scan results for their C&A analysis and based their required deliverable, the C&A analysis report upon this process. The COR staff and FSA staff believed that the C&A contractor met the vulnerability scanning deliverable requirement.

- The Department does not agree with the OIG interpretation on the contract requirements for penetration testing. The contract specifically required penetration testing to leverage vulnerabilities discovered during the scans. Since no vulnerabilities that met the agreed upon definition of 'finding' were discovered, there was nothing to attempt to leverage via penetration testing.

- While the Department is in agreement that the COR did not perform all of his/her duties in conformance with Department policy, the Department is not convinced that the unauthorized changes and direction that occurred is as a result of a fragmented COR monitoring team. As stated previously, all CORs assigned to this contract each had a number of years experience as IT contract CORs.

- The Department concurs that verbal agreements with the contractor presented the possibility of future confusion and/or disagreements; however, these agreements did not result in a reduced level of effort that impacted price. The verbal agreements clarified the original intent of the contract and the level of effort for which we contracted was received.

- The Department does not concur that the verbal agreements regarding the extent of penetration testing for the Tier 4 systems resulted in less assurance for the Department that these high-risk systems were adequately protected against unauthorized access. We believe most Federal civilian agencies do not utilize vulnerability scanning or penetration testing in their C&A reviews. The Department opted for a C&A review that exceeded that employed at the majority of Federal civilian agencies because we wanted to provide a higher level of assurance. We believe that that higher level of assurance was realized.

c. The COR/OCIO staff did not ensure that the CO was informed of changes in key personnel and that the contractor submitted to the CO formal notice and requests for written approval of substitution of key personnel.

The Department concurs with this finding. However, the Department disputes that the level of knowledge of the contractor personnel substituted without the knowledge of the contracting officer may not have equaled that of the designated key personnel upon which the contract award decision was at least partially based. Although the contracting officer was not properly involved with these personnel changes, the C&A project management team did closely review and discuss these changes prior to implementation. The resumes and qualifications were reviewed before personnel changes were made. The level of service and personnel skills and expertise were specifically addressed and monitored. The Department did not receive any reduction in service or quality. For the OIG to infer this is purely speculative in nature.

d. The COR did not document evaluations of contractor-submitted reports or provide written evaluations of the reports to the CO.

The Department concurs with this finding. The C&A contractor delivered the reports; however, the Department acknowledges that the subsequent audit trail of reviews does not exist. The OIG purports that potential problem indicators included in the reports may not have been detected by the COR and in consideration that the contracting officer was not provided evaluations to confirm that reports were being received as required by the contract to take any required action to protect the Government's interest. The Department does not believe that any potential problems were overlooked.

Department Response to OIG Recommendations for Finding No. 1

1.1.a The Department concurs with this recommendation. A customized database has been implemented to assist in tracking deliverables at the requirements level. Requirements checklists have been developed that are used to validate formal acceptance of all deliverables. Formal deliverable acceptance is documented in writing.

1.1.b The Department concurs with this recommendation. The contracting officer is specifically cited throughout the modified PWS as the only authorized individual to make any changes to the contract.

1.1.c The Department concurs with this recommendation. The contracting officer notification of key personnel changes is already in effect.

1.1.d The Department concurs with this recommendation. The COR has already begun documenting contractor reports and submitting the evaluations to the contracting officer.

1.1.e The Department concurs with this recommendation. The COR has already begun building a proper contract file that reflects all information required to carry out the monitoring responsibilities.

1.2 The Department concurs with this recommendation. Several meetings have already taken place beginning in July 2004, to discuss the contract monitoring plan and to clarify roles and responsibilities.

1.3 The Department concurs with this recommendation. Processes are already in place that ensures that any substitution in key personnel follow appropriate procedures.

1.4 The Department concurs with this recommendation. The contracting officer will ensure that any changes in COR responsibilities receive the proper appointment memoranda.

1.5 The Department does not concur with the underlying findings for this recommendation and therefore does not concur with the recommendation. The Department does not concur that incentive payments were made to the contractor improperly, that deliverables were unacceptable, or that payment was made for more than it should have for the work completed. The Contracting Officer had already determined that an opinion is not required from Office of General Counsel.

Finding No. 2 - The Performance Work Statement Did Not Require Sufficient Documentation to Support C&A Recommendations and Decisions

The Department does not agree that the original PWS did not require sufficient documentation to support certification decisions. The documentation requirements in the original PWS were consistent with those in other Federal agencies and based on Federal guidelines to support C&A recommendations and decisions. NIST 800-34 places the emphasis on the System Security Plan and the Security Test and Evaluation (ST&E) plan. The original PWS placed a similar emphasis on these two areas as the basis for the subsequent C&A recommendations and decisions. Thorough and consistent ST&E plans were executed for each of the 10 systems reviewed in this audit.

Department Response to OIG Recommendations for Finding No. 2

2.1. The Department concurs with this recommendation and this action is completed.

2.2. The Department concurs with this recommendation. This action has been implemented with the current contract modification that will be a template for future C&A contracts.

Thank you again for this opportunity to respond. Should you have questions, please contact Glenn Perry, Director, Contracts and Acquisitions Management at (202) 245-6200.