UNITED STATES DEPARTMENT OF EDUCATION
OFFICE OF INSPECTOR GENERAL

AUDIT SERVICES

September 24, 2010

FINAL ALERT MEMORANDUM

TO: Danny Harris
Chief Information Officer
Office of the Chief Information Officer

Thomas Skelly
Acting Chief Financial Officer
Office of the Chief Financial Officer

FROM: Keith West /s/
Assistant Inspector General for Audit

SUBJECT: Implementation of the Managed Security Services Provider Contract
Control Number ED-OIG/L19K0011

While reviewing the Department of Education's (Department) corrective actions in response to the Office of Inspector General's (OIG) Alert Memorandum, "Conflicting Responsibilities Included in the EDNet Contract Performance Work Statement,"[1] we became aware that the Department has not effectively implemented the Managed Security Services Provider (MSSP) contract. Specifically, the Department terminated the initial contract due to contractor performance problems and the subsequent contractor has been unable to provide the level of service required by the contract. As a result, the Department has paid for services it has not received and has still not ensured that its information technology (IT) network is adequately protected. The purpose of this alert memorandum is to bring our concerns to your attention in order to expedite corrective action.

Background

The Department awarded the Education Network (EDNet) contract, effective May 1, 2005, with the goals of improving all services provided to the Department's customers and to lower costs through IT integration. The EDNet contract was structured under the Government-Owned Contractor-Operated IT service model. The EDNet contractor's responsibilities included providing managed services such as server maintenance, messaging (email and Blackberry), and end-user support for hardware and software.

[1] Control Number ED-OIG/L19G0009, dated February 16, 2007

In October 2005, the OIG first reported that the EDNet contractor had conflicting responsibilities because it was responsible for: 1) establishing, installing, configuring, and operating security processes; 2) detecting and reporting any violations in the security processes it established and operated; and 3) reporting such violations and incidents. As a result, in reporting on security violations and incidents, the contractor could be negatively reporting on its own performance in maintaining a secure network. The OIG recommended that the Department consider procuring the services of an independent contractor with the responsibilities of identifying, responding to, and reporting computer security incidents.[2]

OIG followed up on corrective actions in response to the October 2005 report during a subsequent audit of the effectiveness of the Department's management of the EDNet contract.[3] OIG determined that the Department initiated actions to establish a separate contract, but a planned acquisition was cancelled in August 2006. OIG issued an alert memorandum in February 2007 that encouraged the Department to proceed as quickly as possible to eliminate the conflict of responsibilities in the EDNet contract.[4]

In its response to the February 2007 alert memorandum, the Department indicated a revised MSSP procurement with reworked requirements was in progress. The Department was simultaneously procuring IT services to replace the EDNet contract, using a Contractor-Owned Contractor-Operated (COCO) IT service model, under which the contractor is required to provide the total IT infrastructure to support Department employees.[5] In September 2007, the Department subsequently awarded both the Education Department Utility for Communications, Applications, and Technology Environment (EDUCATE) contract and the initial MSSP contract.

The Department Has Not Effectively Implemented the Managed Security Services Provider Contract

Termination of the Initial MSSP Contract

The Department awarded its initial contract for MSSP services to Global Analytic Information Technology Services, Inc. (GAITS) on September 7, 2007 at a fixed cost of $5.1 million for the base year. The acquisition was intended to provide services such as identifying, responding to, and reporting computer security incidents. We noted the Department prepared numerous documents identifying contractor performance problems shortly after award. These included:

- Correspondence between the Department and GAITS during the period September 2007 through November 2007 regarding requirements for its subcontractor[6] to complete system Certification and Accreditation (C&A) and related progress. This included email correspondence from the Department dated October 19, 2007 that identified

[2] *Review of the Department's Incident Handling Program and EDNet Security Controls* (Control Number ED-OIG/A11F0002).
[3] *The Department's Management of the EDNet Contract* (Control Number ED-OIG/A19G0009), dated April 17, 2007.
[4] See Footnote 1.
[5] Includes hardware and software, data centers, networks, etc.
[6] Symantec Managed Security Services

October 30, 2007 as the deadline for Department review and approval of C&A along with correspondence from the contractor dated November 26, 2007 indicating that C&A had not been resolved.

- A show cause notice dated December 3, 2007 that stated that GAITS had failed to meet the 60-day transition period contractual requirement and that the Department was considering terminating the contract for default.
- A stop work order dated February 12, 2008 that required the contractor and its subcontractor to immediately cease work on the contract.
- A memorandum to the contract file dated April 22, 2008 that concluded that GAITS failed to become fully operational by the required date despite being given every opportunity to correct identified performance issues.

Ultimately, the Department took action to terminate the contract for convenience effective April 22, 2008. Based on a review of related documentation and discussions with Department officials, it appeared that there were multiple reasons for the C&A related performance problems and the termination of the initial MSSP contract:

- Department officials with responsibility for contract oversight believed the requirement for C&A was conveyed in its acquisition documents and understood by the contractor. However, a lack of clarity in the MSSP's solicitation documents may have contributed to conflicting interpretations by the contractor and the Department.

  The Contracting Officer's Representative (COR) indicated that GAITS was fully aware of C&A requirements and that GAITS made assertions in its oral presentations prior to award that C&A would be performed on its subcontractor's systems. During discussions conducted during our review a Department official indicated that assertions made during oral presentations were non-binding, but the Department did not believe a written commitment to C&A was needed because language in the acquisition documentation required the contractor to abide by related Department guidance. However, a November 26, 2007 letter from the contractor stated it was experiencing performance delays in part because it did not anticipate having to do C&A work as it was not specifically defined in the Request for Proposal (RFP) or the resulting contract.

  We reviewed the MSSP RFP and found it contained the following clause:

  > Potential offerors are directed to the security requirements under the clause entitled "Information Technology System Security Requirements", ED 307-13. Technical Proposals must include a separate detailed plan for meeting these requirements, including any necessary subcontract applications. Submission of these plans shall serve as certifications of the offerors' full intent for compliance.

  We reviewed ED 307-13 as incorporated in the RFP and found it stated the following:

  > The Contractor and its subcontractors shall comply with Department Security policy requirements as set forth in:

> a. The Statement of Work of this contract;
> b. The Privacy Act of 1974 (P.L.93-579, U.S.C. 552a);
> c. The U. S. Department of Education Handbook for Information Assurance Security Policy, OCIO [Office of the Chief Information Officer]-01 (March 2006); and
> d. The U.S. Department of Education Departmental Directive OM [Office of Management]:5-101, "Contractor Employee Personnel Security Screenings."…

We reviewed the U. S. Department of Education "Handbook for Information Assurance Security Policy," OCIO-01, Section 3.8, dated March 31, 2006, and found it stated the following:

> All Department major applications and general support systems shall be certified and accredited prior to processing any Department information that has security considerations due to its confidentiality, integrity, or availability requirements… All Department IT systems must be accredited at minimum every three (3) years and evaluated annually or whenever there is a significant change to the system's security posture. IT systems that are not major applications shall be certified and accredited as part of their general support systems or shall be combined with other systems.

The MSSP Performance Work Statement (PWS)[7] included the following statement:

> The successful contractor's service facility must demonstrate full and complete compliance with the Departments [sic] security requirements (including Information Assurance Site review/Survey)…

- The contractor's technical proposal included a separate plan for how it would meet security requirements under ED 307-13 as Appendix 2. While this indicated the contractor would comply fully with the requirements of OCIO-01, C&A was not specifically addressed. A separate portion of the technical proposal appeared to indicate GAITS would rely, at least in part, on certifications and audits of its subcontractor to meet security requirements. The proposal specifically stated the following:

  > Processes and Procedures Fully Audited by Trusted Third Parties: Symantec Managed Security Services meet the stringent industry best practices outlined in both the BS7799 certification and SAS70 Type II audit standards. KPMG performs these audits, thoroughly testing Symantec's policies, processes, and procedures to ensure that they conform to the strict requirements of these two industry-respected standards. Symantec is the only Managed Security Services provider to pass these two key audits.

[7] Term used interchangeably with Statement of Work.

- The Department's April 22, 2008 memorandum provided additional information about the cause of the contractor's performance problems and the rationale behind the Department's actions to end the contract. While the memorandum concluded that resolution of performance issues was unlikely, it stated that the Department decided to negotiate a settlement based on termination for convenience of the government. This decision was made because the Department was identified as a "minor contributing factor in the contractor's inability to meet transition milestones." The memorandum stated this was because the Department did not: 1) clearly indicate a requirement for C&A in the solicitation; 2) provide an adjustment to the 60-day transition period once the requirement was clarified; and 3) timely respond to inquiries and requests for meetings GAITS believed were imperative to the transition period progress. The memorandum further indicated that the potential for protracted and costly litigation if the contract was terminated for default was an additional factor in the decision to terminate for convenience.

Ultimately, the Department paid a settlement to GAITS in the amount of $1.5 million to end the contract. The Department concluded the amount was acceptable because it represented an amount that was significantly under the actual costs incurred by the contractor that were allocable to the contract. However, the COR believed the Department received no valuable services for the amount paid, as the contractor primarily completed activities such as planning and scheduling.

Inability of the Current MSSP Contractor to Provide the Level of Service Required

After the Department terminated the GAITS contract, it initiated an additional effort to acquire MSSP services. On August 18, 2008 the Department acquired the services of the Cyber Security Management Center (CSMC) through an Inter Agency Agreement (IAA) with the Department of Transportation (DOT) for a performance period of August 21, 2008 through August 20, 2009, for a total order amount of $3.6M.[8] The Memorandum of Agreement states that the objective of the contract with the CSMC is to "provide continuous monitoring and testing to ensure the EDUCATE contractor(s) delivers real-time detection, assessment, response and remediation related to all relevant cyber incidents." Subsequent to the execution of the agreement, there were numerous indicators of problems with the structure of the agreement and the ability of the CSMC to provide the level of service required.

The COR indicated that since the inception of the contract, CSMC experienced problems obtaining access to the EDUCATE contractor's systems. As a result, CSMC was unable to provide the required services. However, the Department still renewed the IAA with CSMC for the period August 17, 2009 through August 16, 2010 for a total order amount of $5.1M. The COR indicated that the agreement was renewed with the hope that the CSMC would obtain access to the EDUCATE system and the Department would receive the full value of services.

The Deputy Program Manager (PM) indicated he became aware in September 2009 that the Department was not receiving services equivalent to the amount paid to CSMC after

[8] The total funds for the IAA are committed at the time of the agreement execution. DOT CSMC then draws down the necessary funds from the account throughout the year.

familiarizing himself with the agreement and its related performance.[9] In an email sent to the Director of Information Assurance and the COR, dated December 15, 2009, the Deputy PM indicated his dissatisfaction with CSMC's performance. The COR recommended that he draft a notice of action memorandum. However, according to the Deputy PM, the memorandum was drafted and sent to the COR but never sent to CSMC.

Through discussions with Department officials and review of project status reports, we found that CSMC was not able to meet all of its Service Level Agreements (SLA)[10] from the inception of the agreement. Seven of nine COR inspection reports for the period ended January 31, 2010 identified problems with performance of individual SLAs. Problems included items such as the inability to perform (b) (2) , failure to acquire tools necessary to perform penetration testing, lack of feedback on work relating to (b) (2) monitoring and reporting, and lack of documentation from CSMC showing compliance with SLA terms.

In January 2010, the EDUCATE Independent Verification &Validation (IV&V) contractor sent an email to the Director of Information Assurance outlining concerns with CSMC's performance. These included items such as ineffective weekly meetings, ineffective project management by the Department and CSMC, lack of detailed schedules to assess performance, and unclear "ownership." The IV&V suggested several corrective actions, including production of a Service Compliance Matrix that lists the status of each deliverable, documentation of CSMC's efforts in a weekly status report, and requiring CSMC to develop a Work Breakdown Structure of all required items to include who is in charge of actions and what is to be completed. According to the IV&V, some of the recommendations were implemented, but the degree to which they were implemented varied.

The COR prepared a memorandum dated March 15, 2010 that concluded that the Department is not receiving equitable services for the costs incurred. The COR attached a compliance matrix to the memorandum that indicated that CSMC was non-compliant with 11 of the 15 measured performance standards (73 percent) during year two of the agreement. While the attachment showed 10 of the 11 non-complaint areas (91 percent) as having 0 percent compliance, only 2 of the 11 instances of noncompliance (18 percent) were solely attributed to CSMC. The COR further concluded that it was unlikely performance could be improved because of barriers and obstacles presented by the EDUCATE COCO environment. The COR suggested that the IAA be renegotiated to reflect the scope of work CSMC was able to perform and that the Department seek recovery of $2.1M for a portion of the services paid for but not provided. This amount assumes the agreement would be renegotiated as of April 2010 (i.e. so as not to penalize CSMC for year one and the portion of year two prior to renegotiation). The memorandum also indicated the COR had completed market analysis that concluded that common, related services were available in the commercial sector at a substantial cost savings from what was being paid to CSMC. The Deputy PM wrote a memorandum addressed to the COR and Director of

[9] The Deputy PM began working on the DOT CSMC agreement in March 2009.

[10] SLAs are agreements that set expectations between the service provider and the customer. The SLA describes what will be done and how well it will be done, thus providing the basis for measuring, tracking and managing service performance against service levels.

Information Assurance, dated April 15, 2010, that concurred with the conclusions and recommendations noted by the COR.

The inability of the current MSSP contractor to provide the level of service required occurred for several reasons. Numerous individuals, documents, and reports indicated CSMC did not have a level of access to the EDUCATE network that was necessary to fully meet the requirements of the agreement. However, we found that the EDUCATE PWS did include a provision for such access that should have been enforced, as stated in Section C.40(d):

> The government will have a Managed Security Services Provider (MSSP) that is required to perform IV&V on all IT resources, systems, and networks storing, accessing, or transmitting government data. The contractor shall allow all necessary access to the MSSP in performing authorized activities including but not limited to:
> (1) Vulnerability scanning on hosts and networks;
> (2) Access control audits on hosts and networks

We noted a specific concern expressed by the EDUCATE contractor that related to the impact the MSSP contractor's access to the system may have on the EDUCATE contractor's performance with regard to its SLAs. According to the EDUCATE CO, concerns over accessibility were discussed during weekly EDUCATE CO/COR meetings during the life of the CSMC contract. Because the topic was not consistently included on meeting agendas the CO believed the issue was being actively resolved.

In addition, the Department did not always have a structure in place to effectively monitor the performance of the IAA and did not react to concerns identified by key oversight officials. As previously noted, the Department did not assign a Deputy PM until 7 months into the contract and did not timely resolve performance issues identified by its EDUCATE IV&V contractor, progress reports, and internal correspondence.

As a result, the Department paid for a level of service that CSMC was not able to provide and still does not have assurance that its IT network is adequately secured.

According to the COR, the OCIO is planning a revised approach where the Department will perform functions that the CSMC cannot because of network access limitations. The Deputy PM provided OIG with CSMC's proposal for an additional year of support beginning August 11, 2010 for a total cost of $3.1M. The COR stated OCIO has requested $1.5M for tools and software to allow the Department to perform its own testing of the EDUCATE contractor's system and will hire two staff to perform this function.

Recommendations

We recommend that the Chief Information Officer and Chief Financial Officer:

1.1 Formally review and evaluate alternatives for obtaining MSSP services and proceed with a solution that best serves the interests of the Department in a cost effective manner. A

solution should be implemented as quickly as possible to ensure the Department's network is adequately protected.

1.2 In any future acquisitions, ensure key MSSP contract requirements are clearly identified in the RFP and resulting contract.

1.3 Actively enforce the terms of Section C.40(d) of the EDUCATE PWS to ensure adequate access to contractor systems for the performance of MSSP services.

1.4 Establish a process, to include the assignment of an accountable official, for timely resolving issues applicable to the MSSP.

Department Comments

A draft of this memorandum was provided to OCIO and the Office of the Chief Financial Officer (OCFO) for comment. In its response to the draft alert memorandum, OCIO/OCFO generally concurred with our findings, concurred with each of our recommendations, and described corrective actions already taken or planned. OCIO stated it partially concurred that the MSSP contract failed to have a structure to effectively monitor the performance of the IAA, outlining monitoring activities conducted by the COR from the initial IAA deployment. The response is included in its entirety as Attachment 2 to this memorandum.

OIG Response

While we acknowledge that a monitoring structure was in place, we specifically questioned the effectiveness of the structure due to the limited action taken by the Department over a two year period to correct the causes of the identified performance problems.

We conducted our work in accordance with the OIG quality standards for alert memoranda.

Corrective actions proposed (resolution phase) and implemented (closure phase) will be monitored and tracked through the Department's Audit Accountability and Resolution Tracking System.

Alert memoranda issued by the Office of Inspector General will be made available to members of the press and general public to the extent information contained in the memoranda is not subject to exemptions in the Freedom of Information Act (5 U.S.C. § 552).

The publication of this report includes the redaction of information that we have concluded may pose risks to agency regulation or security measures.

For further information, please contact Michele Weaver-Dugan, Director, Operations Internal Audit Team, at (202) 245-6941.

Acronyms/Abbreviations Used in this Report

C&A	Certification and Accreditation
CO	Contracting Officer
COCO	Contractor Owned Contractor Operated
COR	Contracting Officer's Representative
CSMC	Cyber Security Management Center
Department	U.S. Department of Education
DOT	Department of Transportation
EDUCATE	Education Department Utility for Communications, Applications and Technology Environment
FAR	Federal Acquisition Regulation
GAITS	Global Analytic Information Technology Services, Inc.
IAA	Inter Agency Agreement
IT	Information Technology
IV&V	Independent Verification and Validation
MSSP	Managed Security Services Provider
OCIO	Office of the Chief Information Officer
OCFO	Office of the Chief Financial Officer
OIG	Office of Inspector General
OM	Office of Management
PM	Program Manager
PWS	Performance Work Statement
RFP	Request for Proposal
SLA	Service Level Agreements

UNITED STATES DEPARTMENT OF EDUCATION

WASHINGTON, D.C. 20202-_____

September 10, 2010

MEMORANDUM

TO: Michele Weaver-Dugan
Director, Operations Internal Audit Team
Office of the Inspector General

FROM: Danny A. Harris, Ph.D.
Chief Information Officer

Thomas P. Skelly
Delegated to Perform Duties and Functions of the Chief Financial Officer

Subject: Response to: Draft Alert Memorandum Entitled "Implementation of the Managed Security Services Provider Contract" ED-OIG/L 19K0011

Thank you for providing the subject alert memo dated August 23, 2010. The Office of the Chief Information Officer (OCIO) and the Office of the Chief Financial Officer (OCFO) concur with the findings, with noted exceptions. Non-concur comments and stipulations are detailed in specific comments in the body of this memorandum.

Attached is the Department's response, as well as corrective actions, with associated target dates for completion.

OCIO concurs: that some of the issues affecting the Managed Security Service Provider's (MSSP) inability to provide the levels of service as prescribed in the Memorandum of Agreement (MOA) / Inter Agency Agreement (IAA) are the result of the contractual hurdles and challenges posed by the EDUCATE contract vehicle.

OCIO partially concurs: that the MSSP contract failed to have a structure to effectively monitor the performance of the IAA. From the initial IAA deployment, the Contracting Officer's Representative (COR) deployed a Service Level Agreement (SLA) monitoring system, contract line item number charts, contract deliverable tracking inspection reports, and a host of other performance tracking reports. However, due to staffing constraints, a dedicated program manager (PM) was unavailable for the base year and for part of the second year. This staffing issue is being addressed with a GS-15 new hire.

Without the engagement of the Cyber Security Management Center (CSMC), OCIO would not have had the cyber situational awareness of EDUCATE that drove the implementation of our network hardening, Cyber Security Watch activities, the Information Assurance (IA) Discovery initiative and the IA Enhancement Concept of Operations. (b) (2) [redacted]
(b) (2) [redacted]

Response to Recommendations

1.1 *Formally review and evaluate alternatives for obtaining MSSP services and proceed with a solution that best serves the interests of the Department in a cost effective manner.*

OCIO Concurs: The MSSP COR conducted a Cost Benefits Analysis (CBA) on February 23, 2010, (see attachment A). The CBA analyzed commercial services from vendors attached to the General Services Administration (GSA) IT-70 Schedule - with the currently renegotiated IAA (effective August 13, 2010) with the Department of Transportation's Cyber Security Management Center (DOT/CSMC). The analysis reflects a cost savings of several hundred thousand dollars under the five new SLAs. Additional performance metrics have been established for comparison analysis for the OCIO, Contracts and Acquisition Management (CAM) and the Office of the General Counsel (OGC).

The Department has renegotiated the IAA with DOT for MSSP services, effective August 13, 2010, in a one-year agreement/contract. Prior to the award of the FY 11 IAA for EDUCATE's cyber security, an in-depth analysis was conducted, reviewing past services and the OCIO's current capabilities and cyber posture. As a result of OCIO's direct access to the EDUCATE management consoles for anti-virus monitoring; vulnerability scanning; access to audit and log information; technical analysis services from in-house staff; the chartering and implementation of the EDUCATE daily Cyber Security Watch reports; and the on line real-time use of US CERT's Einstein devices, we were able to reduce the services requested in future years. (b) (2) [redacted]
(b) (2) [redacted] as we now have access to the scanning and patching reports for all the servers in the network. The new IAA has dramatically reduced the SLA roster - down to five from ten - and at a reduced level of cost - down to $3.09M/year from $5.1M/year. The new SLAs take into account only those services and deliverables currently available to the MSSP provider by the EDUCATE provider (Perot/Dell).

1.2 *In any future acquisitions, ensure key MSSP contract requirements are clearly identified in the RFP and resulting contract.*

OCIO and OCFO Concur: We have already taken steps to ensure that the FY 11 IAA award we have both clarified our tasks and establish contract line items that are provisioned but not activated until we have full access as required by EDUCATE Section C Paragraph 40, for our Management Security Service Provider.

1.3 *Actively enforce the terms of Section C.40(d) of the EDUCATE PWS to ensure adequate access to contractor systems for the performance of MSSP services.*

OCIO and OCFO concur: Within 30 days of the final alert memorandum OCIO will provide to OCFO the access level necessary for the MSSP contractor to meet the requirements of its contract. Also, within 30 days of obtaining the access level, OCFO will communicate this information to the EDUCATE contractor and ensure this level of access is provided to the MSSP contractor per Section C.40(d) of the EDUCATE PWS.

1.4 *Establish a process to include the assignment of an accountable official for timely resolving issues applicable to the MSSP.*

OCIO Concurs: The OCIO established a chain of accountable officials, which include the MSSP COR, to manage the contract specifications of the agreement and approve and deploy a project plan for the successful review, acceptance, rejection, and remediation of all deliverables of the new MSSP IAA. Further, we now have a full time Project Manager (PM) who is responsible for the management of the daily operations of the agreement and accepting or rejecting services and deliverables. To improve the management of this IAA, the PM has been tasked to develop a new Quality Assurance Surveillance Plan and a Contract Management Plan. In concert with the COR and the PM, the Acting Director of the Information Assurance Services will continue to be responsible for ensuring that this agreement provides enhancements to the cyber security situational awareness. Additionally, the PM shall complete the development of the new documents for review by COR and approval by the Acting Director of IAS by September 29, 2010.

Although OCIO has always had a COR on the IAA, the assignment of a full time PM was lacking due to staffing shortage. The MSSP has had a full-time PM for most of FY 10. Additionally, the Acting Director of IAS will be taking actions to assist the current and future PM for this project in acquiring PM certification.

cc: Phillip Loranger
CISO and Acting Director, Information Assurance Services

James Ropelewski
Acting Director, Contracts and Acquisition Management