

Department of Labor

Office of Inspector General—Office of Audit

Office of the Assistant Secretary
for Administration and Management



Award and Management of Contracts for Encryption Software Were Significantly Flawed

Date Issued: March 31, 2005
Report Number 05-05-005-07-720

BRIEFLY...

Highlights of Report Number: 05-05-005-07-720, to the Deputy Secretary of Labor.

WHY READ THE REPORT

This report discusses issues surrounding the Department of Labor's (DOL) efforts to purchase and implement encryption software, including:

- DOL's award and administration of a sole-source contract to the Meganet Corporation.
- DOL's decision not to use the Meganet software and services, purchased at a cost of \$3.8 million.
- DOL's purchase of Entrust encryption software through a contract with Videla International Corporation.
- The current status of DOL's file and e-mail encryption capability.

WHY OIG DID THE AUDIT

In July 2003, a complainant raised concerns about a contract awarded by DOL to the Meganet Corporation for the purchase of encryption software and services. We initiated a preliminary review.

On August 4, 2003, DOL's Assistant Secretary for Administration and Management (ASAM) referred the Meganet contract to the DOL Inspector General for audit. The ASAM noted that the contract awarded to Meganet differed significantly in scope and value from the proposal reviewed and recommended by DOL's Procurement Review Board (PRB) and approved by the ASAM. In addition, the ASAM stated his concerns that the Meganet software did not perform as expected, that the award of the contract on a sole-source basis might have been inappropriate, and that the price paid by DOL may not have been "fair and reasonable."

READ THE FULL REPORT

To view the report, including the scope, methodology, and full agency response, go to:

<http://www.oig.dol.gov/public/reports/oa/2005/05-05-005-07-720.pdf>

March 2005

AWARD AND MANAGEMENT OF CONTRACTS FOR ENCRYPTION SOFTWARE WERE SIGNIFICANTLY FLAWED

WHAT OIG FOUND

- Significant irregularities existed in DOL's award of a sole-source contract to Meganet, including the failure of the former Deputy CIO to disclose an apparent conflict of interest.
- Overall responsibility for the Information Technology (IT) and procurement functions are delegated to one executive, creating inadequate separation of duties
- The scope of the sole-source contract awarded to Meganet significantly exceeded the procurement proposal that was presented to DOL's Procurement Review Board (PRB) for consideration.
- DOL's decision to abandon the Meganet products, purchased for \$3.8 million, was not supported.

WHAT OIG RECOMMENDS

We recommended that the Deputy Secretary of Labor:

- Remove the procurement function from OASAM and create an independent Acquisition Office that would report directly to the Deputy Secretary.
- Establish a process to independently review and approve decisions to (a) terminate contracts or (b) not use products or services already purchased.

We also recommended that the ASAM:

- Implement controls to ensure that preaward activities are completed before contract execution, including reconciliation of limits recommended by the PRB.
- Emphasize conflict of interest laws and regulations to all employees during annual ethics training, and remind them of the responsibility to report wrongdoing or suspicions of wrongdoing to the OIG.
- Direct IT staff to execute and document a test of the Meganet and Entrust products and determine whether and how to use them in meeting DOL's encryption needs.

DOL responded that it has already made some policy and staffing changes, plans to implement additional controls, and will consider separating the procurement function from program responsibilities.

THIS PAGE INTENTIONALLY LEFT BLANK

Table of Contents

EXECUTIVE SUMMARY	iii
ASSISTANT INSPECTOR GENERAL’S REPORT	1
RESULTS, FINDINGS, AND RECOMMENDATIONS.....	4
FINDING 1 - There Were Significant Irregularities in the Procurement Process Leading to Award of the Meganet Contract	4
FINDING 2 - Scope of the Meganet Contract (and Subsequent Modifications) Varied Significantly from the Proposal Presented to the PRB for Consideration.....	12
FINDING 3 - DOL’s Reasons for Deciding Not to Use the Products Purchased from Meganet Were Not Supported	15
FINDING 4 - DOL Has Spent Millions of Dollars on Encryption Software and Other Products That Are Not Being Used	21
OVERALL AUDIT CONCLUSION.....	23
RECOMMENDATIONS.....	24
EXHIBIT	
A. Timeline of Key Events	31
APPENDICES	
A. Background	35
B. Objectives, Scope, Methodology, and Criteria	39
C. Acronyms and Abbreviations	41
D. Definitions of Key Technical Terms.....	43
E. DOL Response to Draft Report	45

THIS PAGE INTENTIONALLY LEFT BLANK

Executive Summary

We initiated an audit of the Department of Labor’s (DOL) award and management of a contract with the Meganet Corporation (Meganet) to purchase file encryption software and related services. Our interest arose from concerns reported to us by a complainant. Subsequently, the Inspector General received a memorandum from the Assistant Secretary for Administration and Management (ASAM) raising concerns related to this contract.

Our objectives were to determine:

- Was the sole-source contract awarded to Meganet in compliance with government-wide procurement regulations and DOL procurement policies?
- Did DOL provide adequate justification for not using the products purchased through the Meganet contract and, if so, did DOL adequately justify not attempting to recover the \$3.8 million paid to Meganet?
- What is the current status of DOL’s file and e-mail encryption capability?

In many instances, DOL files did not contain adequate documentation to support decisions made and actions taken in awarding and managing the Meganet contract, abandoning use of the Meganet products, and procuring Entrust encryption products. DOL personnel frequently provided conflicting accounts of related events. As a result, we could not always determine the validity or rationale of DOL decisions and actions. More importantly, DOL officials with oversight responsibility for the IT and procurement functions could not demonstrate that their decisions were sound.

We found the following:

1. Delegating responsibility for Information Technology (IT) and procurement functions to one individual – the ASAM – results in inadequate separation of duties and creates an organizational conflict of interest when purchasing IT products and services.
2. There were significant irregularities in the process of awarding the Meganet contract. Specifically, there was (a) no documentary evidence that the need to purchase encryption software was reviewed by DOL’s Technical Review Board (TRB); (b) inadequate documentation of the Information Technology Center’s evaluations of preproposal submissions; (c) no written justification for use of a sole-source contract; (d) a failure of the former Deputy Chief Information Officer to disclose an apparent conflict of interest; and (e) a possible bias in preparing the Statement of Work.

3. Office of the Assistant Secretary for Administration and Management (OASAM) and Office of the Solicitor officials, who at some point became aware of a relationship between the former Deputy CIO and Meganet's Corporate Counsel that may have created an apparent conflict of interest in awarding the Meganet contract, did not refer the matter to the Office of Inspector General (OIG).
4. The scope of the original contract awarded to Meganet included a second product not in the proposal presented to DOL's Procurement Review Board (PRB) and approved by the ASAM as a sole-source procurement. The contract was later modified to add a third product and adjust the quantities available for purchase without further PRB review or approval.
5. In December 2002, DOL entered into a lease agreement with Videla International Corporation to obtain Entrust products for a department-wide Public Key Infrastructure (PKI) solution. Two of these Entrust products, digital signature and e-mail encryption duplicated the functions of products previously purchased from Meganet.
6. The ASAM's stated reasons for deciding not to use the products purchased from Meganet were not supported. Although the ASAM and his staff stated that the Meganet software did not perform as expected in the planned DOL PKI environment, there were no test results or other documentation to support these assertions. Recent OIG tests of the Meganet product VME 2003 indicated that the product functioned in OIG's test environment that was configured to represent the environment described in the contract.
7. DOL obtained large quantities of encryption products at a cost of \$5.4 million without a fully deployed PKI. Neither the Meganet products and services (\$3.8 million) nor the Entrust products and services (\$1.6 million) currently provide benefit to DOL.

CONCLUSION

The Meganet contract was not properly awarded, modified, or managed because of a lack of organizational separation of duties, inadequate oversight, and insufficient internal controls. Furthermore, individuals knowingly made decisions and took actions that violated Government regulations and DOL policies and may not have been in the best operating or financial interests of DOL. As a result, (a) a contract may have been improperly awarded on a sole-source basis, (b) \$3.8 million in Meganet products have gone unused without adequate justification, and (c) DOL spent an additional \$1.6 million (as of December 2004) on Entrust products to satisfy some of the same technical requirements as the unused Meganet products. The OIG believes that until procurement and programmatic responsibilities are properly separated and effective controls put in place, DOL continues to be at risk for the wasteful and abusive practices evident in its handling of the Meganet contract.

RECOMMENDATIONS

We recommend that the Deputy Secretary of Labor:

1. Remove the procurement function from OASAM and create an independent Acquisition Office whose Director would (a) supervise all DOL procurement staff and (b) report directly to the Deputy Secretary.
2. Establish a process for an independent review and approval of decisions to (a) abandon or terminate active contracts or (b) not use products or services already purchased. This review and approval should be made by an individual or group independent of the DOL agency(ies) involved in the purchase or use of the product or service.
3. Remind all DOL employees of their responsibility to immediately report reasonable suspicions of wrongdoing to the OIG.

We also recommend that the Deputy Secretary instruct the ASAM to:

4. Develop and implement procedures to ensure that all required preaward activities (e.g., TRB review, proposal evaluation, etc.) are completed and documented prior to execution of a final contract.
5. Emphasize conflict of interest laws and regulations to all employees during fiscal year 2005 annual ethics training.
6. Develop and implement a procedure to reconcile the terms of PRB approval with the related contract terms before final contract execution.
7. Direct Information Technology Center staff to execute and document the results of a formal test of both the Meganet and Entrust products and determine whether and how to use them in meeting DOL's overall encryption needs or otherwise obtain value to DOL for the costs incurred.
8. Develop a policy and implement controls to limit the quantities of information technology products that are purchased until there is documented evidence that the products are deployable in DOL's system environment.

DOL RESPONSE

In a written response to a draft of this report, the Deputy Secretary stated that some steps had already been taken to correct the procurement problems identified in this report and that additional corrective actions would be implemented. Specifically, he stated that the Department had (a) instituted controls to prohibit expenditures for sole-source contracts that exceeded 10 percent of the amount approved by the PRB and the duration approved by the PRB without prior approval by the Chief

Acquisition Officer; (b) changed the staff closest to the award of the Meganet contract. He also stated that the Department will (c) carefully weigh the reasons provided for recommending the separation of the procurement function from OASAM; (d) establish a policy and procedure for reviewing the termination of substantial or sensitive contracts; (e) remind employees of their responsibility to report suspected wrongdoing to the OIG; and (f) will continue to address conflict of interest rules in its 2005 required ethics training for all employees.

The Deputy Secretary stated that conducting and documenting a formal test of the Meganet products operational capabilities would provide no benefit because recent OMB guidance requires all Federal agencies to use one of three approved PKI service providers. None of these providers uses Meganet encryption software.

OIG CONCLUSION

The response provides sufficient detail to resolve one of the eight OIG recommendations. The other recommendations remain unresolved pending additional or more detailed information concerning planned corrective actions. The OIG does not agree with the Department's position that the recent OMB guidance eliminates any ability to utilize the Meganet products purchased.

U.S. Department of Labor

Office of Inspector General
Washington, DC 20210



Assistant Inspector General's Report

The Honorable Steven J. Law
Deputy Secretary of Labor
U.S. Department of Labor
200 Constitution Ave., N.W.
Washington, DC 20210

In July 2003, a complainant raised concerns about a contract awarded by the U.S. Department of Labor (DOL) to the Meganet Corporation (Meganet) for the purchase of encryption software¹ and services. We initiated a preliminary review. In August 2003, DOL's Assistant Secretary for Administration and Management (ASAM) sent a memorandum to the DOL Inspector General (IG), referring the Meganet contract for audit. The ASAM's memorandum noted that the Meganet contract differed significantly in both scope and value from the proposal reviewed and recommended by DOL's Procurement Review Board (PRB) and approved by the ASAM for a sole-source award. In addition, the ASAM stated his concerns that the Meganet software did not perform as expected, the award of the contract on a sole-source basis might have been inappropriate, and the price paid by DOL may not have been "fair and reasonable."

In early 2001, DOL's Information Technology Center (ITC) identified a need for a commercial-off-the-shelf (COTS) application to encrypt files. To identify companies that could potentially offer products to meet this need, DOL's Office of Procurement Services (OPS) published a Request for Information (RFI). Since 8 of the 15 companies responding to the RFI were small businesses, DOL designated this procurement as a "small business" set-aside. OPS then issued a proposed Statement of Work (SOW) to the eight responding small businesses and asked that each company submit a capability study. Three of the small businesses responded. By evaluating the information provided by these three small businesses, ITC concluded that Meganet was the only respondent capable of meeting the requirements. The former Deputy Chief Information Officer (CIO)² requested that

¹ Technical concepts referred to in this report are defined in Appendix D.

² DOL's former Deputy Chief Information Officer was also the Director of DOL's Information Technology Center. The individual who served in this dual capacity during the award of the Meganet contract left DOL employment on March 28, 2003. Her successor (referred to in this report as the current Deputy CIO) also holds these dual responsibilities.

the PRB review and recommend approval of a sole-source contract award to Meganet. The Procurement Review Board recommended, and the ASAM approved, the award of a sole-source contract to Meganet to “obtain a product and service for the encryption process needed for the Employee Computer Network” at an estimated cost of \$950,000.

In February 2002, OPS awarded Meganet a sole-source contract to purchase (a) file encryption software and services and (b) digital signature software and services at a potential cost between \$1.08 million and \$4.03 million. Four months later (June 2002), OPS modified the contract to add a third product and services for e-mail encryption. This modification also reduced the maximum quantities available under the contract for each product and service. There is no evidence that the PRB reviewed, or that the ASAM approved, use of this sole-source contract to purchase digital signature or e-mail encryption products.

In March 2003, after spending \$3.8 million for products and services under the Meganet contract, the ASAM decided not to install any of the software purchased from Meganet. Based on information provided to him by his staff, the ASAM concluded that the Meganet products would not function properly in DOL’s environment. The current Deputy CIO informed Meganet in a September 2003 letter that DOL did not intend to use the Meganet products.

Despite the assertion that the Meganet products purchased would not function properly, the ASAM also decided not to attempt to recover any of the funds paid to Meganet. An attorney from DOL’s Office of the Solicitor (SOL) advised the Office of Inspector General (OIG) that it could not defend terminating the contract for default because the language of the contract was “murky” and it was not clear that Meganet had not fulfilled all of its obligations under the contract.

In December 2002, DOL began procuring encryption software and hardware by Entrust through a lease agreement with Videla International. Two of the Entrust products duplicated the functions – digital signature and e-mail encryption – of products previously purchased from Meganet. As of December 2004, DOL had spent \$1.6 million on products and services under the Videla contract. However, neither the Meganet nor the Entrust encryption products are currently being widely used in DOL because an essential part of the overall security solution, DOL’s Public Key Infrastructure (PKI), is still being piloted by a limited number of users. [See Exhibit A for a timeline of key events, and Appendix A for more background information.]

The Office of the Assistant Secretary for Administration and Management (OASAM), ITC, OPS and the PRB provided very limited documentation to support the procurement and contracting decisions and related actions in these matters. Personnel involved in awarding the contract to Meganet, abandoning the Meganet products, and acquiring the Entrust encryption products, presented different, and often conflicting, accounts of events. These matters remains under OIG review.

Our objectives were to determine:

- Was the sole-source contract awarded to Meganet in compliance with government-wide procurement regulations and DOL procurement policies?
- Did DOL provide adequate justification for not using the products purchased through the Meganet contract and, if so, did DOL adequately justify not attempting to recover the \$3.8 million paid to Meganet?
- What is the current status of DOL's file and e-mail encryption capability?

Results, Findings, and Recommendations

OBJECTIVE: Was the sole-source contract awarded to Meganet in compliance with government-wide procurement regulations and DOL procurement policies?

No. The process followed in awarding the sole-source contract to Meganet did not comply with government-wide procurement regulations or DOL procurement policies. There were significant irregularities as described in Findings 1 and 2. These irregularities cast doubt on the appropriateness of awarding this contract to Meganet on a sole-source basis. By delegating responsibility for Information Technology (IT) and Procurement functions to one individual, the ASAM, the resultant lack of separation of duties facilitated this lack of compliance with procurement requirements.

Finding 1 - There Were Significant Irregularities in the Procurement Process Leading to Award of the Meganet Contract

There were numerous irregularities in the process used by DOL to award a sole-source contract to Meganet. Specifically, there was (a) no documentary evidence that the need to purchase encryption software was reviewed by DOL's Technical Review Board (TRB); (b) inadequate documentation of ITC's evaluations of pre-proposal submissions; (c) no written justification for use of a

sole-source contract; (d) a failure of the former Deputy CIO to disclose an apparent conflict of interest; and (e) a possible bias in preparing the SOW. Individually, and collectively, these irregularities cast doubt on the appropriateness of awarding this contract to Meganet on a sole-source basis.

No Documentary Evidence that DOL's TRB Reviewed the Need for Encryption Software

There was no documentation that the need for encryption software was presented to, reviewed by, or approved by the TRB as required by DOL policy. Therefore, there is no assurance that the encryption software requirement was properly defined in relation to DOL's overall IT structure.

Department of Labor Manual Series (DLMS) 9, Chapter 200, *DOL Guide to IT Capital Investment Management*, May 2000, states:

The TRB provides IT investment analysis and recommendations for above threshold (\$5 million and above annually) **and crosscutting initiatives** to the [Management Review Council] for approval. [Emphasis added.]

It further states,

Technology that is new to the Department or sets new technological direction for an Agency or the Department must be presented to the TRB for review.

Examples of crosscutting initiatives in the *Guide* include matters of interoperability, infrastructure, sensitive and high-visibility initiatives, and instances where several agencies have similar IT requirements. The need for encryption software, which the Meganet contract was aimed at fulfilling, was a crosscutting initiative based on all of these criteria. It was also a new technology within DOL. Therefore, it should have been reviewed and approved by the TRB regardless of the financial value of the investment.

The Contracting Officer's Technical Representative (COTR) for the Meganet contract stated that the requirement was presented to and discussed by the TRB prior to awarding the contract to Meganet. The former Deputy CIO, who was Chair of the TRB at the time of the procurement, also stated that the requirement for file encryption was reviewed by the TRB. However, our review of TRB meeting minutes for the period April 2000 through February 2003, found no mention of file encryption requirements, the Meganet products, or the Meganet contract.

Inadequate Documentation of ITC's Evaluation of Preproposal Submissions

ITC did not adequately define or document its evaluation of preproposal submissions by potential offerors. Therefore, there is no assurance that Meganet actually was the only (or best) small business capable of meeting ITC's file encryption requirement.

On May 2, 2001, DOL published an RFI concerning its file encryption requirements. Since eight of the responses to the RFI were small businesses, DOL designated the file encryption procurement as a "small business set-aside." On June 14, 2001, DOL mailed a SOW to these eight small businesses inviting each potential offeror to submit a "capability statement, qualifications, and references" for review. This mailing was a presolicitation notice as defined in the FAR (Subpart 15.202). Three of the eight small businesses provided responses. One submission was immediately judged to be "non-responsive." The other two submissions were subjected to a technical evaluation based on a point system. However, DOL did not

clearly communicate the evaluation factors to the potential offerors nor was documentation of the method and basis of these evaluations available for our review. Specifically, we noted that:

- The notice provided to potential offerors on June 14, 2001, did not clearly identify the evaluation factors as required by FAR.
- The evaluation score sheets contained no supporting rationale for the point values assigned to the various evaluation criteria for each proposal.
- The evaluation score sheets were unsigned and undated.
- Two sets of score sheets had conflicting results.

These deficiencies prevented us from determining whether Meganet was properly identified as the sole responsible small business capable of meeting DOL's requirements.

FAR Section 15.202 states

The presolicitation notice should identify the information that must be submitted and the criteria that will be used in making the initial evaluation. Information sought may be limited to a statement of qualifications and other appropriate information. . . .

While the SOW provided to potential offerors in the June 14, 2001, mailing identified several broad technical requirements for the file level encryption application needed by DOL, it did not identify specific evaluation factors to be used in assessing responses received. For example, the evaluation score sheets we were provided, that were used in assessing submitted responses, contained six "ease of use" factors. Although the need to "demonstrate ease of use" was included in the SOW provided to the potential contractors, no specific evaluation criteria were defined.

When interviewed by OIG auditors, the former Deputy CIO stated that technical evaluations of responses from two contractors – Meganet and Systems Plus – were performed. She explained that she assigned this responsibility to two of her staff and subsequently reviewed the resulting evaluation forms. She stated that Systems Plus's proposal was not a COTS product; therefore, she concluded that Meganet was the only responsive small-business submission. The COTR for the Meganet contract also told OIG auditors that signed copies of the evaluations were prepared and forwarded to the Procurement Office and that additional signed copies of the evaluations were maintained in ITC's official file and in the COTR's personal file.

The COTR alleged that she provided ITC's official file and her personal Meganet file to the ASAM's Special Assistant and the CIO's Special Assistant, at their request, for review. According to the COTR, when the files were returned, several documents (including the signed copies of the evaluations, a chronology of events, and personal notes) had been removed from the files. The ASAM's Special Assistant and the

CIO's Special Assistant acknowledge requesting and reviewing these files, but deny removing any of their contents.

During the course of the audit, a former ITC staff member that we interviewed stated that he completed and signed product evaluation forms. He also stated that the evaluation materials were bundled and provided to the COTR. However, our review located only two sets of unsigned, undated evaluation forms in the files OASAM provided to us.

The unsigned, undated response evaluations demonstrated that two small businesses submitted responses that were each scored on two sets of score sheets. In one set of evaluations, Meganet's proposed product received zero points because it was deemed incompatible with the version of the Windows operating system being used by DOL. The product proposal from Systems Plus received 75 points.

One of the evaluators subsequently sent an e-mail to each of the two companies requesting information in response to specific follow-up questions. Based on their original responses and the additional information they provided in response to the e-mail follow-up questions, the companies were then subjected to a second set of evaluations. However, this time the evaluation criteria were modified by removing the following question from the original criteria:

14. *Does the product line (vendor) already have a product within the ECN? (Implying existing maintenance, historic credibility, past experience)*

With the removal of this item on the second set of evaluations, Meganet received 95 points and Systems Plus received 90 points. Had this item not been removed from the evaluation criteria, Systems Plus would have received an additional five points (for a total of 95) creating a tie with Meganet. Neither set of evaluations contains any narrative or other supporting information that would explain why the evaluator(s) assigned given point values to various criteria. There is also no documentation to explain why item #14 was removed from the second evaluation criteria.

Since neither the evaluation criteria definitions nor the methodology used to measure the responses against the evaluation criteria were documented, we could not assess whether the evaluation results were consistent or fair. Accordingly, we could not determine the validity of the evaluation results contained in DOL's files nor the judgment that Meganet was the best or only potential provider.

No Written Justification for Use of a Sole-Source Award

OASAM did not provide us with the documentation required by government-wide and DOL regulations to justify the award of a contract to Meganet on a sole-source basis. As a result, there is no assurance that DOL was justified in limiting competition in meeting its encryption requirement.

The FAR provides seven limited exceptions to the award of government contracts through other than “full and open competition” and describes the content of the justification required for using each of these exceptions. The ASAM’s letter approving the use of a sole-source contract cited FAR 6.302-1, which states: “only one responsible source and no other supplies and services will satisfy agency requirements,” as the appropriate exception to full and open competition for the Meganet contract.

FAR 6.302-1(d)(1) states

Contracts awarded using this authority shall be supported by the written justifications and approvals described in 6.303. . . .

FAR Section 6.303-1 states,

A contracting officer shall not commence negotiations for a sole-source contract . . . or award any other contract without providing for full and open competition unless the contracting officer . . . justifies, if required in FAR 6.302, the use of such action in writing [and] certifies the accuracy and completeness of the justification. . . .

Further, DLMS 2, Section 836 (f) 1 states,

ASAM approval is not the final determination for use of ‘other than full and open competition.’ Before a proposed acquisition instrument can be awarded with ‘other than full and open competition,’ the justification for such a noncompetitive action must be prepared in accordance with FAR 6.303. . . . The justification in FAR 6.303 [is] in addition to the PRB review and ASAM approval.

DOL’s COTR stated that the sole-source contract was justified because Meganet submitted the only proposal that offered a COTS product, as required. This assertion was also contained in the materials provided to the PRB for review. However, DOL’s contract file for the Meganet contract contained nothing to support this assertion or to satisfy either the FAR or DLMS requirements. As a result, there is no way for the OIG or anyone else to review or validate DOL’s reasoning for pursuing a noncompetitive award to Meganet.

Failure to Disclose an Apparent Conflict of Interest

The former Deputy CIO violated Federal regulations and DOL policy when she participated in the process that led to a sole-source contract award to Meganet without disclosing an apparent conflict of interest. It is also of concern to us that, after the Department became aware of a relationship between the former Deputy CIO and Meganet’s Corporate Counsel, the matter was not referred to the OIG.

In November 2001, the former Deputy CIO initiated a request to award a sole-source contract to Meganet. As required by DOL's procedures, she signed form DL1-490, *General Information for the Procurement Review*, certifying that she had no present or prior business, personal, or financial relationship with Meganet. However, the attorney who was employed as Corporate Counsel for Meganet (and still holds that position today) had represented the former Deputy CIO in a personal legal matter in calendar year 2000, prior to Meganet submitting its proposal to sell encryption software to DOL. In addition, the attorney informed the OIG that, in August and November 2001, while the Meganet procurement was under way, he reviewed draft reports relating to the same personal legal matter on behalf of the former Deputy CIO.³ The former Deputy CIO did not disclose this relationship to DOL procurement officials.

Further, in October and November of 2000, the former Deputy CIO corresponded with Meganet's Corporate Counsel (via e-mail) regarding encryption-related topics. As part of this correspondence, the former Deputy CIO provided editing suggestions on a proprietary Meganet document discussing Virtual Matrix Encryption (VME). The product documentation provided with the encryption software tested by the OIG (VME Office 2003, Version 2.0.22.12) states that it uses VME.

When interviewed by the OIG, the former Deputy CIO initially denied knowing that the attorney who represented her in 2000 was associated with Meganet prior to the contract award. However, after we provided her with copies of the e-mail messages discussed in the previous paragraph, the former Deputy CIO admitted knowing, prior to the contract award, of his connection to Meganet. She then explained that this attorney was not representing her in any personal legal matters at the time of the contract award; therefore, she did not believe there was any conflict of interest.

According to FAR Subpart 3.101,

The general rule is to avoid strictly any conflict of interest or even the appearance of a conflict of interest in Government-contractor relationships.

In addition, DLMS 2, Section 835 states,

The program official responsible for an 'other than full and open competition' request or a request for contract advisory and assistance services shall, . . . explain any past or existing business or personal relationships with the proposed recipient or certify that none exist.

Further, 5 CFR 2635.502(a) states,

³ This attorney also represented the former Deputy CIO in a separate personal legal matter in calendar year 2003, after the Meganet contract award.

Where an employee knows that a particular matter involving specific parties is likely to have a direct and predictable effect on the financial interest of a member of his household, or knows that a person with whom he has a covered relationship is or represents a party to such matter, and where the employee determines that the circumstances would cause a reasonable person with knowledge of the relevant facts to question his impartiality in the matter, the employee should not participate in the matter unless he has informed the agency designee of the appearance problem and received authorization from the agency designee in accordance with paragraph (d) of this section.

The former Deputy CIO had an apparent conflict of interest, based on having employed Meganet's Corporate Counsel as her personal attorney before the contract award. Corresponding with Meganet's Corporate Counsel and providing technical editing advice on encryption-related topics shortly before DOL began its search for encryption products, further brings into question her ability to be unbiased in the contract award process. This apparent conflict of interest is of greater concern in light of the sole-source nature of the contract award. Under these circumstances, based on Section 835 of DLMS 2 and 5 CFR 2635.502(a), the former Deputy CIO's prior attorney-client relationship with an attorney, who was employed by and represented Meganet throughout the entire contract award process, precluded the former Deputy CIO from participating in the Meganet procurement unless she had disclosed the relationship to appropriate DOL officials and received prior approval to participate as provided in 5 CFR 2635.502(d). The former Deputy CIO failed to disclose the relationship or seek approval of her participation in the Meganet matter.

An additional concern is raised by the fact that the ASAM's August 4, 2003 memorandum referring the Meganet contract to the IG for review, while raising several concerns about the appropriateness of the sole source contract award to Meganet, did not include any reference to the relationship between the former Deputy CIO and Meganet's Corporate Counsel. In an e-mail sent to five SOL attorneys on July 31, 2003, the ASAM's Special Assistant states:

I have crafted the attached referral to the oig (we did not feel it was appropriate to mention the **apparent** conflict of interest involving [the Meganet Corporate Counsel's] representation of [the former Deputy CIO] and meganet).

DLMS 8, *Audits and Investigations*, Paragraph 713 states

- (a) All DOL employees are responsible for: (1) Promptly reporting . . . to their supervisor or the OIG, information that they reasonably believe indicates wrongdoing. . . .

- (b) DOL Agency Heads are responsible for: (1) Ensuring that all allegations of wrongdoing received by supervisors or managers within the Agency are reported promptly to the OIG.

DLMS 8, Paragraph 704(a)(6) defines “wrongdoing” as including “conflict of interest.”

When interviewed by the OIG in late 2004, two senior SOL attorneys stated that they were aware of the relationship between the former Deputy CIO and Meganet’s Corporate Counsel. Both attorneys stated that there was not sufficient information to establish that a conflict of interest existed. Therefore, they did not believe that the matter required referral to the OIG pursuant to DLMS 8. Despite their conclusion, some concerns remained about this relationship, because the attorneys also stated that it was their understanding that the information about the relationship would be informally communicated to the OIG in some fashion. However, this informal communication never occurred.

The OIG believes that the information available to the Department provided a reasonable basis to suspect possible wrongdoing and, therefore, should have been referred to the OIG pursuant to DLMS 8.

Possible Bias in Preparing the Statement of Work

The COTR stated that she could not recall the extent of her involvement in writing the SOW used to solicit proposals. However, the OIG obtained an e-mail sent by the COTR to the former Deputy CIO on June 5, 2001, stating, “I actually wrote [the Statement of Work] by taking it ou[t] of the Meganet book you gave me.” When shown this e-mail, the COTR stated that the “Meganet book” was a publicly available brochure that she probably only used to obtain definitions of terms with which she was unfamiliar. On June 14, 2001, the completed SOW was mailed to Meganet and seven other small businesses requesting capability statements. The possibility that the SOW was based on a Meganet product brochure, or other Meganet materials, raises a serious concern that the SOW may have been prepared in a manner that unfairly favored Meganet’s products.

Inadequate Separation of Duties Facilitated Noncompliance

Currently in DOL, overall responsibility for the IT function and the procurement function are both delegated to one individual – the ASAM. This creates an organizational conflict of interest whenever a procurement action involves IT products or services. Similarly, an organizational conflict of interest occurs whenever a procurement action is undertaken in support of OASAM’s operational mission. OMB Circular A-123, *Management Accountability and Control*, states:

Key duties and responsibilities in authorizing, processing, recording, and reviewing official agency transactions should be separated among individuals.

The ASAM has been delegated procurement and contracting authority in Secretary's Order 4-76. Specifically, the ASAM is responsible for prescribing procurement policies and procedures, procuring property and services, and resolving questions and interpretations of Federal Procurement Regulations.

In addition, the ASAM serves as DOL's CIO. The Clinger-Cohen Act (40 U.S.C. 11315) established the position of CIO in each Federal department. In DOL, the CIO reports directly to the Secretary and Deputy Secretary and "has [Information Resource Management] duties as his or her *primary* duty . . . [emphasis added]" (Secretary's Order 3-2003). Currently, this dual role not only conflicts with the requirement that IRM duties be the primary duty of the CIO, but it also creates a potential conflict whenever DOL purchases IT products and services. The lack of adequate separation of duties increases the risk that operational needs and desires will override sound procurement practices. Likewise, the same organizational conflict of interest exists whenever a procurement action is taken to meet the operational needs of any OASAM component.

Finding 2 - Scope of the Meganet Contract (and Subsequent Modifications) Varied Significantly from the Proposal Presented to the PRB for Consideration

The scope of the original contract with Meganet, effective February 1, 2002, included a second product not in the proposal presented to DOL's PRB on November 26, 2001, and approved by the ASAM on December 5, 2001, as a sole-source procurement. The contract was modified on June 6, 2002, to add a third product and adjust the quantities available for purchase

without further PRB review or approval. Without PRB review, there is no assurance that Meganet was the only available provider of these additional products.

Original Contract Terms Exceeded the Scope of the Proposal Approved by the PRB

On November 15, 2001, the former Deputy CIO sent a Procurement Review package to the ASAM requesting the use of a sole-source contract to obtain "a product and service for the encryption process needed for the Employee Computer Network [ECN]." The ASAM, in turn, submitted the proposal to the PRB to review and make a recommendation regarding the appropriateness of awarding a sole-source contract. The request described plans to "obtain software necessary to perform file level encryption, to provide the installation of the software, and to provide the maintenance on an as needed basis" for the ECN (approximately 1,300 computers). The estimated value of the contract was \$950,000. On

November 26, 2001, the PRB recommended that the ASAM approve a sole-source contract to Meganet. A memorandum, dated December 5, 2001, from the ASAM to the Deputy CIO, gave approval to pursue a sole-source contract to Meganet.

A DOL contracting officer entered into a sole-source contract with Meganet, effective February 1, 2002, to purchase (1) a file level encryption application, (2) a digital signature application, and (3) related maintenance services. The minimum quantity to be purchased for each of the three items was 4,800 with a maximum purchase quantity of 18,000 each. Based on the negotiated fixed price per item, the contract had a total value between \$1.08 million and \$4.03 million over the 3-year term of the contract. The inclusion of a second product (i.e., digital signature application) and the increased quantities (from 1,300 to potentially 18,000) exceeded the proposal presented to the PRB for consideration. As a result, the dollar value of the contract was potentially four times the estimate presented to the PRB.

According to the ASAM, it was December 2002 when he and the PRB became aware of the variance between the contract proposal submitted for PRB review in November 2001 and the terms of the actual contract awarded in February 2002. In December 2002, the former Deputy CIO had forwarded a request to the PRB to increase the maximum product quantities allowed in the existing contract. The increases were intended to allow the United States Department of Agriculture (USDA) to purchase Meganet products under the DOL contract. When the ASAM noted the difference between the existing contract and the proposal originally submitted to the PRB in 2001, he withdrew the new request for PRB consideration.

In November 2001, when the original Meganet contract proposal was presented for PRB review, DLMS 2, Section 836 (a) stated,

It is the policy of DOL that all requests to award acquisition or assistance instruments, or modifications to acquisitions or assistance instruments are subject to review by the PRB, which recommends approval or disapproval to the Assistant Secretary.

At the time of the Meganet contract award, DLMS 2 did not address the PRB's authority to establish scope limitations (e.g., dollar amount, duration) on a contract. In the case of the Meganet contract, the PRB's function was only to make a recommendation regarding the request to award a contract on a sole-source basis.

The OPS Director, in a memorandum to the PRB, stated that he considered that the PRB had determined Meganet was the sole-source for encryption products and services for the ECN, and that the \$950,000 presented to the PRB was an estimate, not a cap. Therefore, the contracting officer did not feel bound by any dollar limit identified by the PRB. The OPS Director also stated in the memorandum, however, that in hindsight, the PRB should have been informed that the negotiated contract price considerably exceeded the estimated amount in the PRB's approval memorandum. The contract's COTR stated that the PRB was informed that the cost of the contract was an estimate when the proposal was discussed. The PRB did not

indicate that \$950,000 was a contract ceiling nor that the COTR needed to return to the PRB for additional approval if a higher cost was negotiated. Therefore, neither OPS nor the COTR believed it was necessary to go back to the PRB for approval at the time the contract was entered into and modified. However, the addition of a new product to the planned contract would constitute a modification that should have been subject to PRB review. In the OIG's judgment, the differences could have been identified if DOL's process had required reconciliation between the proposal reviewed by the PRB and the actual contract terms prior to the contract award.

The ASAM indicated that as a result of the Meganet contract, revisions were made to DLMS 2 in May 2003. Language was added to allow dollar and term limits to be established on contracts reviewed by the PRB. DLMS 2, Section 836 I (3) was amended to state:

If approved, the ASAM's decision memorandum will specify the approved project duration and funding, as appropriate. A new request to the PRB will be required if an Agency Head wishes to exceed either the approved funding amount by 10 percent (or other percent as specified by the ASAM) or extend project duration beyond the approved period.

The new policy still does not specify a method for reconciling the contract terms reviewed by the PRB and those included in the final contract award.

Meganet Contract Scope Modified After Award Without PRB Review

On June 6, 2002, DOL modified the original Meganet contract. The maximum quantities for the original two products -- file encryption (VME 2000) and digital signature (VME Sign) -- were reduced from 18,000 to 10,000, and a third product for e-mail encryption (VME Secure Mail) was added along with related licensing and administrative support services. The minimum purchase quantity of this new product was 4,800 units with a maximum purchase quantity of 10,000 units. The COTR and OPS believed it was not necessary to obtain approval from the PRB for this change because the total dollar value of the original contract had not increased.

The ASAM and some members of the PRB believe that the original contract of February 2002 and the modification in June 2002 should have been resubmitted to the PRB for review because of changes in the scope of the contract. As previously cited, DLMS 2 Section 836 (a) required that modifications were "subject to review by the PRB." These changes should not have been made without PRB review and the ASAM's approval. In addition, DOL's desire to purchase the second and third products was never announced in the marketplace. Therefore, there is no way to determine whether other potential contractors (including small businesses) could have competed with Meganet to fill these additional needs.

OBJECTIVE: Did DOL provide adequate justification for not using the products purchased through the Meganet contract and, if so, did DOL adequately justify not attempting to recover the \$3.8 million paid to Meganet?

No. The two reasons given by DOL for not using the Meganet products were not supported. Although Meganet's products were not certified by the National Institute of Standards and Technology (NIST) as complying with Federal Information Processing Standard (FIPS) 140, Meganet was in the process of obtaining the required NIST certification. DOL provided no documented test results to support their assertion that the products would not function in DOL's environment. OIG's testing indicated that the VME 2003 product provided to OIG from DOL functioned in OIG's test environment designed to represent the environment described in the contract. The Deputy Assistant Secretary for Administration and Management (DASAM) provided inadequate oversight to scrutinize and resolve conflicting information about the ability to implement the Meganet products.

Finding 3 - DOL's Reasons for Deciding Not to Use the Products Purchased from Meganet Were Not Supported

DOL's decision not to install the products purchased under the Meganet contract was not supported. The CIO's Special Assistant raised concerns about the viability of the Meganet products after being hired by DOL in mid-December 2002. This was 10 months after awarding the contract and after DOL had received and paid for more than

\$3 million of products under the contract. In late December 2002, as part of an overall PKI acquisition plan, DOL entered into an agreement to lease Entrust encryption products (a GSA Schedule vendor) through a contract with Videla International Corporation, a re-seller of Entrust products.⁴ Some of these Entrust products duplicated the functionality of the previously purchased Meganet products.

The ASAM and members of his staff stated to OIG auditors that the Meganet products did not perform as expected. Specifically, they cited two reasons for abandoning implementation of the Meganet products: (1) the products did not meet mandatory certification requirements and (2) the products would not function within DOL's proposed PKI structure. However, they provided no documentation to support these assertions. On September 29, 2003, the current Deputy CIO sent Meganet a letter stating that DOL did not intend to use any of the products purchased from Meganet.

⁴ Other than determining that Entrust products were available from the GSA schedule, our audit did not focus on determining whether this procurement complied with the FAR.

In spite of the asserted product deficiencies, and based on advice from an SOL attorney, DOL decided not to pursue recovery of any of the funds paid to Meganet. In an interview with OIG auditors, the SOL attorney characterized the contract terms as “murky” and could not conclude that Meganet had not met its contract obligations.

Product Deficiencies Alleged by DOL

According to the contract COTR, ITC staff did not indicate any major problems with the Meganet products ordered. However, in December 2002, DOL contracted with Videla to obtain Entrust encryption software as part of an overall PKI solution plan. According to the COTR, when she questioned the apparent duplication of the products in the Meganet and Videla contracts, the CIO’s Special Assistant and the ASAM’s Special Assistant expressed concerns about installing the Meganet products. Specifically, the Special Assistants questioned whether Meganet’s products were properly certified by NIST for compliance with FIPS 140. The COTR also indicated that the Special Assistants stated that Meganet’s products would not work with DOL’s proposed PKI unless some information technology issues were resolved.

The former Deputy CIO stated that, to her knowledge, the CIO’s Special Assistant was the only individual that had ever raised concerns about whether the Meganet products worked. In fact, according to the former Deputy CIO, prior to the CIO’s Special Assistant’s involvement (December 2002), the ITC had thoroughly and successfully tested and was preparing to deploy the Meganet software. They were waiting only for DOL’s PKI to be completed and operational.

By March of 2003, DOL had ordered and received the maximum quantities of all products under the Meganet contract at a total cost of \$3.8 million. However, in a May 8, 2003 letter, DOL rejected payment of the final invoice from Meganet in the amount of \$664,300. The letter cited five specific deficiencies as the basis for refusing payment:

- 1) the cryptographic module was not validated to comply with NIST FIPS;
- 2) the encryption tool did not implement the “3DES” encryption method”
- 3) the Meganet product was not fully interoperable with DOL’s PKI;
- 4) the digital signature module was not certified to comply with NIST FIPS; and
- 5) the digital signature tool did not implement the “DSA” digital signature method.

According to the letter, each of these items was required in the “original statement of work.”

The ASAM’s office led a series of meetings (March 28, 2003, April 10, 2003, and May 15, 2003) to discuss concerns about the Meganet products, including the specific deficiencies listed in the May 8, 2003 letter. DOL officials (including

representatives from the ITC, OPS, and SOL) participated in some or all of these meetings along with Meganet representatives.

Meganet and DOL officials differed in their assessments of the results of these meetings. According to Meganet's Corporate Counsel, Meganet staff successfully responded to all operational concerns raised by DOL at these meetings. To support this conclusion, he pointed out that DOL rescinded its earlier rejection and paid the final invoice in full (plus interest) on June 2, 2003. However, the ASAM stated that the parties were unable to resolve the deficiency concerns to DOL's satisfaction. He explained that payment of the final invoice was made because SOL staff believed that DOL's failure to reject earlier shipments of the Meganet products precluded it from filing for breach of the contract. On September 29, 2003, the current Deputy CIO sent Meganet a letter stating that DOL did not intend to use any of the products purchased or order any further products through the contract with Meganet.

Based on the information available for our review, the five deficiencies cited in the May 8, 2003 letter do not provide a sound basis for abandoning DOL's \$3.8 million investment in the Meganet products that had been purchased. The SOW contained in the awarded contract did not state a requirement for the "3DES" encryption method (deficiency #2). Although the SOW provided to vendors with DOL's request for capability statements did contain this requirement, it was unexplainably omitted from the contract SOW. We found no testing results or other documentation to support DOL's assertion that the "3DES" method was absent from the Meganet products.

The language in the contract SOW did not specifically require use of the "DSA" digital signature method (deficiency #5). Instead, it required that the product "support Digital Signatures as follows in IAW [in accordance with] FIPS PUB 186-1." FIPS PUB 186-1 (December 15, 1998) identifies either the Digital Signature Algorithm (DSA) or another algorithm (RSA) as appropriate and specifically states that both do not have to be implemented.⁵ According to Meganet officials, their product included RSA services. Again, DOL provided no documentation to demonstrate that the products lacked this capability.

The contract SOW did require that the Meganet products demonstrate "integration [with] the agency's standard PKI solution . . ." (deficiency #3). However, DOL provided no documentation or other support for its claim that the Meganet products did not operate with its PKI solution. In fact, since DOL only began defining its PKI Functional Requirements in May 2002 and is still running its proposed PKI solution in a limited pilot test, it is unclear how DOL would have determined the lack of performance of the Meganet products against its PKI environment.

⁵ Although cited in the contract SOW, at the time of the contract award FIPS 186-1 was not the current standard. FIPS 186-2, effective July 27, 2000, superseded FIPS 186-1 and allowed the use of any of three different algorithms in digital signature products – DSA, RSA, or ECDSA.

Although we agree that FIPS establish certain mandatory standards for all cryptographic and digital signature modules used by federal agencies, the contract SOW contains only references to FIPS 180-1 and 186-1. We found no language in the contract SOW that identifies other pertinent standards (e.g., FIPS 140-2) or specifies the need for NIST certification (deficiencies #1 and #4). To avoid any ambiguity, the contract should have identified all requirements either through specific language or specific citation to other federal laws or regulations. As with other deficiencies cited by DOL, it provided no evidence or documentation to support its assertion of non-compliance.

DOL assertions that Meganet's products did not possess required NIST certifications are discussed in detail in the following section.

NIST Certification Was Pending and Likely to Be Approved

The CIO's Special Assistant stated that the Meganet software was not certified by NIST as complying with FIPS 140, *Security Requirements for Cryptographic Modules*. FIPS 140 is a technical standard that any cryptographic product must meet before it can be placed on a Federal Government information technology system. At the time of the contract award, Meganet's products did not have their own NIST certification. However, when DOL officials raised this issue, Infogard, a laboratory accredited by NIST to perform cryptographic validation testing, wrote a letter to the former Deputy CIO on Meganet's behalf. The March 25, 2003, letter stated that Infogard was in the process of testing Meganet's encryption product and planned to recommend that Meganet's product be issued FIPS 140 certification. The letter further stated that Infogard did not "anticipate any critical issues that would prevent [Meganet's products] from being validated by NIST." In addition, Meganet argued that it met the certification requirement since its product incorporated (without change) a Microsoft module that did have NIST certification. It had provided DOL with correspondence from a NIST official supporting this interpretation. On January 27, 2005, Meganet received NIST Certificate #505 validating that its VME Crypto Engine complied with FIPS 140-2.

The CIO's Special Assistant stated that the absence of this certification prevented DOL from using the Meganet products. However, DOL was informed that the required NIST certification was in process and likely to be approved. DOL also has reason to believe that the NIST certification requirements had been met through the incorporation of the Microsoft module. Since DOL already had invested \$3.8 million in the purchase of these products, it seems prudent that it would have worked with Meganet to overcome this certification concern rather than immediately abandoning the Meganet products and services based on this issue.

Meganet Products Could Operate in DOL's System Environment at the Time of the Contract Award

The CIO's Special Assistant and the ASAM's Special Assistant on the one hand, and ITC officials on the other, provided conflicting opinions about whether the Meganet products did or did not function properly in DOL's IT environment. In addition, Meganet officials claimed that they had developed applications and demonstrated their product's operability to DOL technical staff. However, we found no documentation to support any of these assertions. Specifically, we found no documentation that DOL had tested the Meganet products at all. Subsequently, OIG technical staff were able to demonstrate the functionality of the Meganet software in a test environment that represented the DOL environment as described in the contract.

The CIO's Special Assistant stated that Meganet's products were not compatible with DOL's needs and required modifications because they were not based on "standard modules." The CIO's Special Assistant further stated that Meganet officials claimed that their product code was proprietary and refused to reveal it to DOL. According to the CIO's Special Assistant, Meganet attempted to demonstrate its product by incorporating Microsoft modules that were available at no charge to make the Meganet product compatible with DOL's proposed PKI. The CIO's Special Assistant said the product still did not work. We were not provided with any documentation or other corroborating evidence to support the assertions by the CIO's Special Assistant.

Section C.3.1 Task #1 (file level encryption application testing, demonstration, and evaluation) of the contract with Meganet states:

The Contractor shall conduct integration testing and demonstration of the application or provide the proposed application directly to the technical point of contact listed in this SOW. The application testing, demonstration, and evaluation shall be performed in the Government's on-site Test, Evaluation and Certification Center (TECC) located in room N1301, Francis Perkins Building. The application must demonstrate successful integration and operation on the DOL standard Windows NT workstation before being accepted.

Both ITC staff and Meganet officials stated that testing of the Meganet products was performed. However, no documentation of these tests or their results was found. The testing reportedly consisted of a demonstration of the products by Meganet staff on a computer in the DOL lab. Meganet personnel opened, closed, encrypted, and decrypted files. Meganet personnel discussed how the products functioned, and DOL personnel explained how the product should operate in the DOL environment. It is not clear which version of software was tested, but Windows 2000 was running in the lab at the time the software was demonstrated. ITC and Meganet officials stated that they believe the product would have worked in DOL's environment.

The former Deputy CIO stated that DOL had conducted formal, thorough testing of the Meganet products and that she was aware of no reasons why the products

would not have performed satisfactorily in DOL's environment. She also stated that the test results had been documented as required. Specifically, she recalled that the file of test documentation was substantial in size and included the test plan (7-10 pages), printouts of before and after "screen shots," and event logs.

Meganet officials stated that their staff had worked with DOL ITC staff to test the Meganet encryption products and make sure they would run in the proposed DOL PKI system environment. According to Meganet's Chief Executive Officer, Meganet developed an application to test their products in a stand-alone environment. They also developed four applications that simulated PKI to test their products, since DOL's PKI was not in place. Although Meganet officials claim that these tests demonstrated that their products worked in DOL's environment, they also could not provide any documented test results to support their assertions.

In an effort to resolve these conflicting assertions, OIG obtained copies of the product from DOL for testing. On November 9, 2004, OIG technical staff, assisted by Meganet personnel, was able to demonstrate the functionality of Meganet's VME Office 2003 product. The OIG was able to determine that the Meganet VME 2003 product functioned in a networked e-mail test environment as described in the contract. OIG was able to (a) successfully install the Meganet software on three laboratory computers, one running Windows NT 4.0 Server software and the other two running Windows NT 4.0 Workstation software; (b) demonstrate functionality of the VME Office 2003 on the three computers; and (c) successfully test the encryption and decryption of e-mails transmitted through the OIG Computer Lab Microsoft Exchange Server.

OASAM's decision not to use the Meganet products because the products could not function in DOL's IT environment at the time of the contract is not supported.

Inadequate Supervision and Oversight

The DASAM was aware that the former Deputy CIO had, prior to her departure from DOL in March 2003, argued that the Meganet products worked and could be implemented. Nonetheless, when the issue of formally severing DOL's relationship with Meganet was raised with the DASAM in September 2003, he did not question the assertions by other OASAM staff that the Meganet products neither worked nor had adequate certification to be implemented. Nor did he raise these issues with the ASAM; instead, he allowed the action to proceed. Overall, although the DASAM was the direct supervisor of the former, current, and interim Deputy CIOs throughout the time period addressed in this report, there is no indication that the DASAM took an active supervisory role in the process of awarding the contract to Meganet, modifying the contract, or otherwise managing the contract

OBJECTIVE: What is the current status of DOL's File and e-mail Encryption Capability?

Although DOL has spent \$5.4 million on encryption products, maintenance and support services, and PKI related hardware from two contractors (Meganet and Videla), there is no file or e-mail encryption capability widely implemented throughout DOL because DOL's PKI, an essential part of the overall security solution, has not yet been widely deployed. A PKI Pilot Project, involving a limited number of DOL users, is ongoing. Department-wide implementation of this capability may not occur until the end of Fiscal Year (FY) 2005.

Finding 4 - DOL Has Spent Millions of Dollars on Encryption Software and Other Products That Are Not Being Used

DOL has obtained large quantities of encryption software from two different vendors, but has not yet deployed the products. DOL abandoned the Meganet encryption software, purchased at a cost of \$3.8 million, and has no plans to install these products. DOL has also entered into an agreement to lease Entrust encryption

software and PKI related hardware at a total cost of \$2.4 million over 3 years. As of December 2004, DOL had paid \$1.6 million of this total. However, the Entrust encryption software purportedly cannot be deployed department-wide because the related PKI is still in a pilot status. As a result, DOL is not benefiting from the \$5.4 million it has spent.

Encryption Software Purchases

DOL has obtained thousands of licenses for encryption software since February 2002, although it did not have a fully deployed PKI framework in which to utilize these products. From February 2002 through March 2003, DOL purchased 10,000 units each of file encryption, e-mail encryption, and digital signature software from Meganet. Including the support services purchased with these products, DOL paid Meganet \$3.8 million. In December 2002, it began leasing Entrust encryption products through an agreement with Videla. From December 2002 through December 2004, DOL obtained 40,000 licenses to use Entrust's e-mail encryption and digital signature software. Including the PKI related hardware and maintenance services purchased with these products, DOL had paid Videla \$1.6 million.

Status of DOL's PKI Solution Pilot

Before DOL can deploy and benefit from all the encryption products it has purchased, it needs a fully deployed PKI. However, DOL did not begin its PKI Solution Pilot until April 1, 2004, more than 2 years after purchasing its initial quantity of encryption software from Meganet and more than 15 months after beginning to procure Entrust encryption products from Videla.

Based on information provided by DOL management, 52 employees, including 7 OIG employees, are participating in the pilot. The objective of the pilot is to demonstrate PKI capabilities in a specific application and provide an opportunity for users and administrators to gain actual experience using the PKI. Lessons learned and other data were scheduled to be collected and documented through December 31, 2004. Deployment of the PKI solution includes the approval and publication of a regulation in the Code of Federal Regulations. Therefore, DOL estimates that full deployment may not be completed until the end of FY 2005.

Nevertheless, DOL had obtained licenses for concurrent use of 40,000 Entrust PKI certificates, e-mail encryption and digital signature software to enable use of these certificates, and related hardware and maintenance from Videla at a cost, as of December 2004, of \$1.6 million. When combined with the \$3.8 million of products purchased through the Meganet contract, DOL has expended a total of \$5.4 million on encryption products and PKI hardware, which are currently not widely deployed.

In addition, since DOL originally procured the Entrust products through the Videla contract, changes in the Federal PKI architecture have reduced the number of licenses and certificates required by DOL. DOL is working with Videla to try and transfer 15,000 licenses and certificates to another Federal agency.

Given the ongoing nature of DOL's PKI Solution Pilot, it was unreasonable for DOL to have obtained large quantities of encryption licenses and certificates. While limited quantities could be procured for use in the pilot effort, large-scale obligations should have been delayed until the PKI solution was complete and the encryption software was widely deployable.

Overall Audit Conclusion

The Meganet contract was not properly awarded, modified, or managed because of a lack of organizational separation of duties, inadequate oversight, and insufficient internal controls. Furthermore, individuals knowingly made decisions and took actions that violated Government regulations and DOL policies and may not have been in the best operating or financial interests of DOL. As a result, (a) a contract may have been improperly awarded on a sole-source basis, (b) \$3.8 million in Meganet products have gone unused without adequate justification, and (c) DOL spent an additional \$1.6 million (as of December 2004) on Entrust products some of which satisfy the same technical requirement as the unused Meganet products. The OIG believes that until procurement and programmatic responsibilities are properly separated and effective controls put in place, DOL continues to be at risk for the wasteful and abusive practices evident in its handling of the Meganet contract.

Recommendations

We recommend that the Deputy Secretary of Labor:

1. Remove the procurement function from OASAM and create an independent Acquisition Office whose Director would (a) supervise all DOL procurement staff and (b) report directly to the Deputy Secretary.
2. Establish a process for an independent review and approval of decisions to (a) abandon or terminate active contracts or (b) not use products or services already purchased. This review and approval should be made by an individual or group independent of the DOL agency(ies) involved in the purchase or use of the product or service.
3. Remind all DOL employees of their responsibility to immediately report reasonable suspicions of wrongdoing to the OIG.

We also recommend that the Deputy Secretary instruct the ASAM to:

4. Develop and implement procedures to ensure that all required preaward activities (e.g., TRB review, proposal evaluation, etc.) are completed and documented prior to execution of a final contract.
5. Emphasize conflict of interest laws and regulations to all employees during FY 2005 annual ethics training.
6. Develop and implement a procedure to reconcile the terms of PRB approval with the related contract terms before final contract execution.
7. Direct ITC staff to execute and document the results of a formal test of both the Meganet and Entrust products and determine whether and how to use them in meeting DOL's overall encryption needs or otherwise obtain value to DOL for the costs incurred.
8. Develop a policy and implement controls to limit the quantities of information technology products that are purchased until there is documented evidence that the products are deployable in DOL's system environment.

DOL RESPONSE

The OIG provided a draft of this report to DOL management for review and comment. The Deputy Secretary's written response to the draft report, dated March 18, 2005, is summarized below and presented in its entirety in Appendix E. As a result of the written response and separate discussions with DOL officials after

we had issued the draft report, we made technical clarifications in the report where appropriate.

In its written response, DOL management stated that the OIG report was thorough, confirmed their concerns about the Meganet contract, and offered constructive recommendations to prevent future contracting problems. They committed to continuing to assess and take appropriate actions to enhance changes that they have begun in the contracting program. Specifically, DOL management addressed each recommendation as follows:

Recommendation 1 – The Deputy Secretary agreed to carefully weigh the OIG’s rationale for recommending that the procurement function be organizationally separated from OASAM in relation to the procedural and personnel changes that OASAM has already instituted.

Recommendation 2 – The Deputy Secretary concurred in principle with this recommendation and directed the ASAM to (a) revise the Department’s procurement policies to ensure an independent review prior to the termination of substantial or sensitive contracts and (b) set an appropriate threshold for reviewing decisions not to use products or services that have already been purchased.

Recommendations 3 and 5 – The Deputy Secretary stated that the Office of the Solicitor discusses how to avoid conflicts of interest in its required ethics seminars. To implement our recommendation, he agreed that SOL’s 2005 ethics training would continue to address an employee’s responsibility to report wrongdoing to the OIG and the rules governing conflict of interest. Further, he stated that appropriate reminders would be sent to employees.

Recommendations 4, 6, and 8 – The Deputy Secretary stated that the Department had already taken steps to substantially address these recommendations by (a) revising DOL policy on sole-source contracts to require approval of the Chief Acquisition Officer if actual spending exceeded the dollar amount approved by the PRB by more than 10 percent or the contract term exceeded the duration approved by the PRB; (b) limiting, through the information technology governance structure, purchases of IT products prior to documenting that the products are deployable in the Department’s system environment; and (c) reinforcing its policy requiring that preaward activities be completed and documented prior to execution of a final contract. He further stated that the Department had made significant changes among the personnel most closely involved in the Meganet procurement, including the Deputy CIO, IT staff that worked with the Deputy CIO, and the senior procurement official.

Recommendation 7 – The Deputy Secretary summarized a perceived contradiction within the report’s findings. He stated that while the report criticizes the Department’s award of a contract to Meganet, it also questions the Department’s decision to set aside the contact and “appears to explicitly endorse Meganet’s

technical capabilities – relying heavily on representations made by the former Deputy CIO and top Meganet officials.” He further questioned the OIG’s testing of the Meganet products “assisted by Meganet personnel.” Finally, he argued it would be doubtful that implementing the OIG’s recommendation to complete a formal test of the Meganet products would provide significant value and benefit to the Department. Citing recently issued requirements from the Office of Management and Budget (Memorandum M-05-05, dated December 20, 2004), the Deputy Secretary stated that all Federal agencies are now required to use one of three approved providers for PKI services. He stated that none of the three currently approved providers uses Meganet’s encryption software.

OIG CONCLUSION

Based on the information contained in the Deputy Secretary’s written response to the draft report, Recommendation 3 is resolved. To resolve each of the other recommendations, we need a more complete and detailed description of planned corrective actions. Our specific assessment of the Deputy Secretary’s response to each recommendation follows.

Recommendation 1 – The Deputy Secretary committed to “carefully weigh” the reasons for this recommendation. This recommendation is unresolved pending a final decision regarding removal of the procurement function from OASAM.

Recommendation 2 – The stated action does not address both aspects of this recommendation. The ASAM has been directed to revise the Department’s policy to ensure a review for “termination of substantial or otherwise sensitive contracts.” However, the response does not include a corrective action for reviewing decisions to not use products or services already purchased. This recommendation is unresolved pending an action plan related to the review of decisions not to use products or services already purchased.

Recommendations 3 – The Office of the Solicitor will address employees’ responsibility to report wrongdoing to the OIG in the required 2005 ethics training. In addition, appropriate reminders will be sent to employees. This recommendation is resolved and will be closed based on the Department providing evidence that these actions have occurred.

Recommendation 4 – The Department has “reinforced its policy requiring that pre-award activities are completed and documented prior to execution of any final procurement contract.” However this recommendation is unresolved until (a) the OIG receives specific information on how this reinforcement was accomplished and (b) the Department defines procedures or internal controls to assure that program and procurement personnel comply with policy requirements. As an example, the Department might consider implementing a checklist of preaward requirements that would be signed off by a senior procurement official prior to final contract execution.

Recommendation 5 – The Department stated that the SOL already discusses how to avoid conflicts of interest in its annual ethics seminars and will continue to address the subject in its 2005 training. However, this recommendation is unresolved pending more specific information describing how SOL will emphasize the conflict of interest laws and regulations in this year’s training.

Recommendation 6 – The Department has not developed and implemented procedures to reconcile the terms of PRB approval with the related contract terms before final contract. This recommendation is unresolved until the Department defines procedures or internal controls to assure that program and procurement personnel comply with any contract limits recommended by the PRB and established by the ASAM.

Recommendation 7 – We see no conflict in our report. We reported that the Department’s procedures were flawed and poorly documented. Therefore, its actions did not assure that it made the appropriate decisions in awarding the contract to Meganet and later abandoning the products purchased. The OIG does not endorse the Meganet products or assert that they can satisfy the Department’s requirements. We recommend that the Department make this determination through formal, documented testing of the Meganet products. If this testing determines that the Meganet products cannot be used to benefit the Department, the recommendation further requests an action plan to identify possible options to recover some or all of the investment in these products.

We disagree with the Department’s position that the December 20, 2004, OMB directive eliminates the possibility of using the Meganet products. First, a technical supplement, issued by the General Services Administration on March 3, 2005, states that compliance with the OMB directive can be achieved in either of two ways: (1) by cross-certifying an agency’s certification authority with the Federal Bridge or (2) by purchasing PKI services from one of the approved Shared Service Providers. Second, there are encryption needs that do not rely on PKI (e.g., file encryption). In fact, this was the originally stated requirement of the Meganet procurement action. Finally, PKI services do not utilize encryption software; rather encryption software utilizes PKI services. Since Meganet’s products currently work with at least one of the three shared service providers available through the General Services Administration program (Verisign), it may be possible to use one or more of the Meganet products purchased and still comply with the OMB directive.

This recommendation is unresolved pending the Department’s (a) plan to formally test the Meganet and Entrust products, (b) determination of whether and how best to use all encryption products purchased to date, and (c) pursuit of options to obtain value for products purchased but not deployed.

***Award and Management of Contracts for
Encryption Software Were Significantly Flawed***

Recommendation 8 – The Department stated that its information technology governance structure “limits purchases of IT products prior to obtaining documentation that the products are deployable.” This recommendation is unresolved pending more specific information about how the existing structure assures that purchases are limited prior to evidence that they can be deployed.



Elliot P. Lewis
December 22, 2004

Exhibits

THIS PAGE INTENTIONALLY LEFT BLANK

Timeline of Key Events

Date	Event
05/02/2001	DOL publishes “sources sought” notice for file encryption products in <i>Commerce Business Daily</i> .
06/14/2001	DOL’s ITC sends a request for quote and capabilities study to eight small businesses.
11/26/2001	DOL’s PRB reviews request to award a sole-source contract to Meganet; estimated contract value is \$950,000.
12/05/2001	The ASAM approves awarding a sole-source contract to Meganet.
02/01/2002	DOL awards sole-source contract to Meganet; original contract value is between \$1.1 and \$4 million.
02/05/2002	DOL approves first invoice for \$613,200 to Meganet.
06/06/2002	DOL modifies Meganet contract scope to add new products and services; no PRB review.
12/04/2002	The former Deputy CIO requests expansion of Meganet contract to include quantities requested by USDA.
12/2002	The CIO’s Special Assistant begins employment at DOL.
12/24/2002	DOL enters into agreement with Videla to purchase Entrust encryption products.
02/11/2003	The ASAM withdraws request to the PRB for modification of Meganet contract based on the CIO Special Assistant’s recommendation.
03/2003	The ASAM makes decision not to use Meganet products.
03/28/2003	The former Deputy CIO leaves DOL employment.
06/02/2003	DOL pays final invoice for \$664,300 to Meganet. Total contract payments equal \$3.8 million.
07/24/2003	Complainant raises concerns about Meganet contract to OIG.
07/31/2003	The ASAM’s Special Assistant sends an e-mail to several SOL attorneys. The e-mail contains a proposed memo for their review from the ASAM to the IG referring the Meganet contract for review. In the e-mail, the ASAM’s Special Assistant states that it is inappropriate to mention the former Deputy CIO’s apparent conflict of interest to the IG.
08/04/2003	The ASAM sends a memo to the IG referring the Meganet contract for possible review by the OIG.
09/29/2003	The current Deputy CIO sent a letter to Meganet stating that DOL will not be using Meganet products.

THIS PAGE INTENTIONALLY LEFT BLANK

Appendices

THIS PAGE INTENTIONALLY LEFT BLANK

Background

On July 24, 2003, we received allegations from a complainant concerning a contract that DOL had awarded to Meganet for the purchase of encryption software for file and e-mail security. As a result, we began gathering preliminary information on the contract.

On August 4, 2003, DOL's Assistant Secretary for Administration and Management (ASAM) sent a memorandum to the DOL Inspector General (IG), referring the Meganet procurement and contract for audit consideration. In the memorandum, and a subsequent discussion with OIG auditors, the ASAM raised three issues that had come to his attention about the sole-source contract awarded to Meganet:

1. The terms of the actual sole-source contract awarded to Meganet varied significantly from those presented to the PRB for review and approved by him.
2. Other contractors might have been able to provide products to meet DOL needs at a lower price than Meganet. Thus, the Meganet contract may have been improperly awarded on a sole-source basis.
3. DOL had decided not to use the products purchased from Meganet.

The IG acknowledged the ASAM's referral in a memorandum on August 7, 2003, noting that the OIG was already looking into aspects of this procurement as a result of a complaint received.

History of Meganet Contract Award

In May 2001, DOL published a "sources sought" notice in the *Commerce Business Daily* to identify companies that could provide commercial off-the-shelf software to perform file level encryption. This requirement was to support the implementation of the Government Paperwork Elimination Act (GPEA) by providing confidentiality and authentication capabilities for stored data. DOL required that the software be compatible with its PKI and any applications used by the general public (e.g., Microsoft Office 2000 and Outlook).

In May 2001, DOL's Information Technology Center (ITC) determined that eight of the fifteen responses received were from small businesses. As a result, DOL decided to limit the procurement to small businesses.

In June 2001 DOL requested that each of the responding small businesses provide a capabilities study. Three of the companies responded to this request; one was

***Award and Management of Contracts for
Encryption Software Were Significantly Flawed***

disqualified because it did not provide the detailed capability information required. Subsequently, two ITC officials completed technical evaluations of proposals submitted by Meganet and Systems Plus. Only Meganet was determined to have an off-the-shelf product ready for distribution.

After requesting and obtaining approval from the A/S for Administration and Management, DOL awarded a contract to purchase file encryption and digital signature software and support services to Meganet on a sole-source basis effective February 1, 2002. Subsequent to the original award, DOL modified the Meganet contract to allow the purchase of an additional (third) product – e-mail encryption software.

In December 2002, DOL entered into an agreement with Videla International Corporation (Videla) to lease Entrust products including software for file encryption and digital signature.

By March 2003, DOL had ordered and received the maximum quantities (10,000 units of each product) allowed under the Meganet contract at a total cost of \$3.8 million.

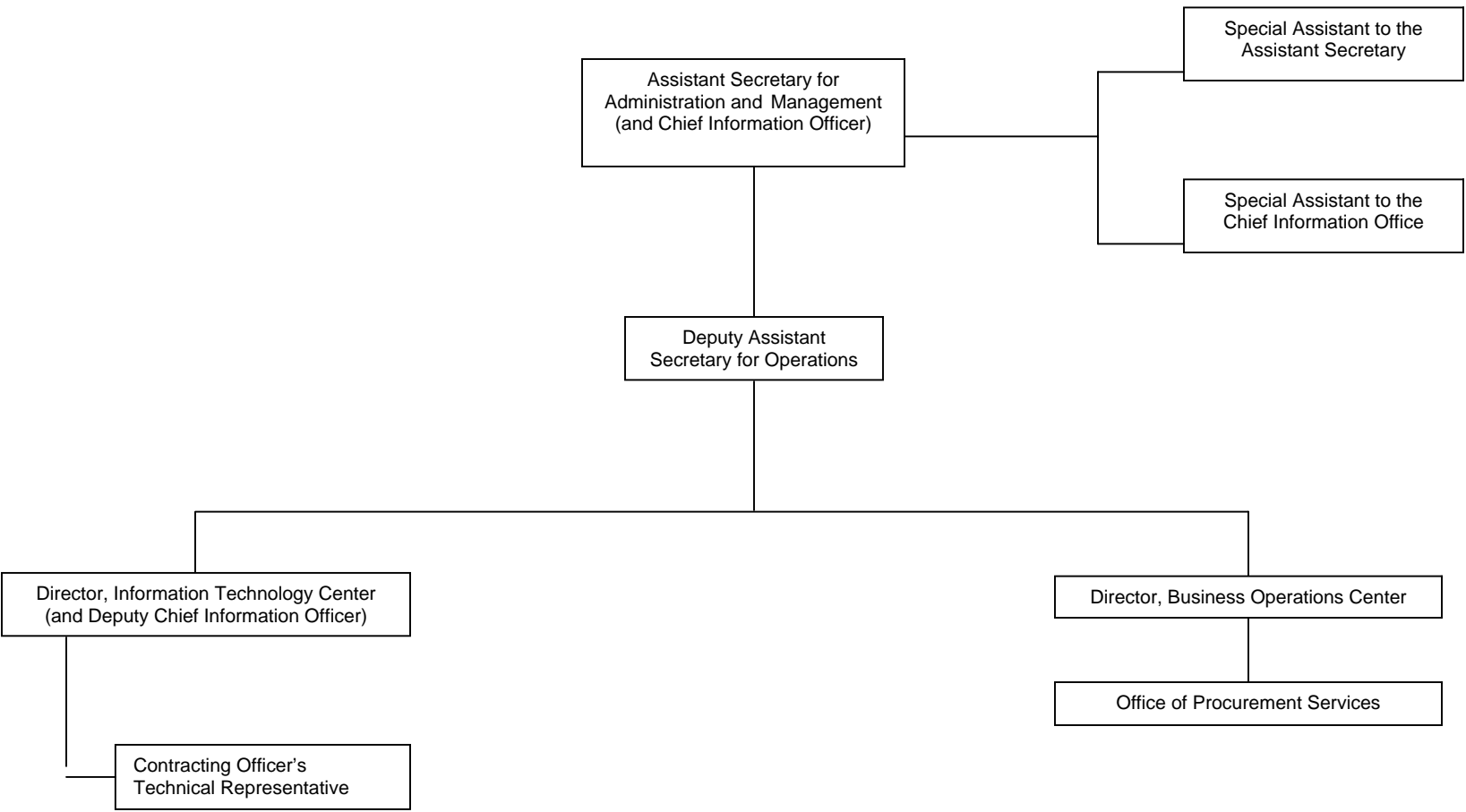
In September 2003, DOL notified Meganet by letter that it did not intend to implement any of the Meganet products purchased and that it would not make any additional purchases under the existing contract.

As of December 2004, DOL had paid Videla \$1.6 million to use 40,000 Entrust PKI certificates, e-mail encryption and digital signature software to enable use of these certificates, and related hardware and maintenance.

Key Participants

Several DOL personnel were involved in the award and administration of the Meganet contract, the decision not to implement the Meganet software, and the procurement of Entrust encryption software through the Videla contract. During the relevant timeline, some individuals left DOL, others joined DOL, and still others changed job responsibilities. The following chart is presented to assist in understanding the organizational roles of these individuals.

Organization Chart
DOL Office of Assistant Secretary for Administration and Management (OASAM)
Procurement and Information Technology Functions Only



THIS PAGE INTENTIONALLY LEFT BLANK

Objectives, Scope, Methodology, and Criteria

Objectives

Our objectives were to determine:

- Was the sole-source contract awarded to Megamet Corporation (Megamet) in compliance with government-wide procurement regulations and DOL procurement policies?
- Did DOL provide adequate justification for not using the products purchased through the Megamet contract and, if so, did DOL adequately justify not attempting to recover the \$3.8 million paid to Megamet?
- What is the current status of DOL's file and e-mail encryption capability?

Scope

The focus of the audit was the appropriateness and adequacy of DOL's award and management of Contract # J-9-M-2-0012. This contract was a sole-source award to Megamet to provide commercial off-the-shelf encryption software, licensing, and maintenance. The contract was effective on February 1, 2002, for a 3-year period.

Methodology

OIG auditors completed the objectives by (a) reviewing pertinent Federal and DOL contracting regulations and policies, (b) reviewing and analyzing all available documentation related to the award and management of the Megamet contract, and (c) interviewing all appropriate DOL and contractor officials and staff involved in either the award or management activities. Due to the lack of available documentation and the conflicting testimonial evidence received, OIG auditors obtained sworn statements from selected individuals with knowledge of the contract award and management activities.

Our audit was performed in accordance with generally accepted Government Audit Standards issued by the Comptroller General of the United States.

Criteria

18 U.S.C. Section 208
18 U.S.C. Section 216
5 CFR 2635.502
Federal Acquisition Regulation
Secretary's Order 1-2000
Secretary's Order 3-2003
Secretary's Order 4-76
DLMS-2
DLMS-8, Chapter 700
DLMS-9, Chapter 200
DOL's Guide to IT Capital Investment Management

Acronyms and Abbreviations

ASAM	Assistant Secretary for Administration and Management
CIO	Chief Information Officer
COTR	Contracting Officer's Technical Representative
COTS	Commercial-Off-the-Shelf
DAEO	Designated Agency Ethics Officer
DLMS	Department of Labor Manual Series
DOL	Department of Labor
ECN	Employee Computer Network
FAR	Federal Acquisition Regulation
FIPS	Federal Information Processing Standards
FY	Fiscal Year
IG	Inspector General
IT	Information Technology
ITC	Information Technology Center
Meganet	Meganet Corporation
NIST	National Institute of Standards and Technology
OASAM	Office of the Assistant Secretary for Administration and Management
OIG	Office of Inspector General
OPS	Office of Procurement Services
PKI	Public Key Infrastructure
PRB	Procurement Review Board
RFI	Request for Information
SOL	Office of the Solicitor
SOW	Statement of Work
TECC	Test, Evaluation and Certification Center
TRB	Technical Review Board
U.S.C.	United States Code
USDA	United States Department of Agriculture
VME	Virtual Matrix Encryption

THIS PAGE INTENTIONALLY LEFT BLANK

Definitions of Key Technical Terms

Decryption

The process of transforming encrypted data back to its original form so that it can be understood.

Digital certificates

The digital equivalent of an ID card used in conjunction with a public key encryption system.

Digital signature

An electronic signature that is used to authenticate the identity of the sender of a message or the signer of a document. A digital signature can also be used to ensure the original content of the message or document was not altered after it was signed.

Digital signature application

Software that allows a user to digitally sign documents.

E-mail encryption software

Software used to protect the confidentiality of e-mail messages by encrypting and decrypting the e-mail between sender and receiver.

Encryption

The process of transforming information from plain text into a format that cannot be easily understood by unauthorized persons.

Encryption application

Application that allows for encryption and decryption of data.

File encryption

To encrypt a file (data, text, etc.) in order to protect its contents from unauthorized access.

License

A permission code, received from a software developer, which allows the user to gain access to a particular version of software (sometimes called a “registration code”).

Public Key Infrastructure

A framework for creating a secure method for exchanging information based on public key cryptography. The foundation of a PKI is the certificate authority (CA), which issues digital certificates that authenticate the identity of organizations and individuals over a public system such as the Internet. The certificates are also used to sign messages, which ensures that messages have not been tampered with.

Response to Draft Report

**Award and Management of Contracts for
Encryption Software Were Significantly Flawed**

U.S. DEPARTMENT OF LABOR
OFFICE OF THE DEPUTY SECRETARY
WASHINGTON, D.C.
20210

March 18, 2005

The Honorable Gordon S. Heddell
Inspector General
U.S. Department of Labor
Washington D.C. 20210

Gordon:
Dear Mr. Heddell:

I appreciate the opportunity to comment on the Office of the Inspector General's (OIG) audit report concerning the award and management of certain contracts for encryption software – a procurement which began in 2001 and was brought to the OIG's attention by a complainant in July 2003 and by detailed memorandum from the Assistant Secretary for Administration and Management (ASAM) in August 2003.

I would like to give further careful consideration to the recommendations included in your audit report, but make the following initial observations and decisions:

Your first recommendation contemplates the complete removal of the procurement function from the Office of the Assistant Secretary for Administration and Management (OASAM), and the creation of a new acquisition office reporting directly to the Office of the Deputy Secretary. I will carefully weigh the reasons provided for this recommendation, while taking into account the substantial management and procedural protections – as well as high-level personnel changes – that have been instituted by OASAM since the events that gave rise to the OIG's audit.

I concur in principle with Recommendation 2, which calls for an independent process to review and approve decisions to terminate active contracts, or not use products or services that already have been purchased. Such a process could add a measure of oversight that would strengthen the Department's contracts management. It would need to differentiate between terminations due to faulty performance by the contractor and terminations for the convenience of the government, and set an appropriate threshold for reviewing decisions not to use products or services that have been purchased. To this end, I have asked the ASAM to revise the Department's procurement policies to ensure such a review for termination of substantial or otherwise sensitive contracts.

Recommendations 3 and 5 of the OIG audit report urge the Department to reinforce with staff the requirements of conflict of interest laws and regulations, as well as the need to report reasonable suspicions of such conflicts to the OIG. These recommendations flow from the OIG's concerns about the appearance of a conflict of interest with respect to the former Deputy CIO's business relationship with Meganet's Corporate Counsel, which could have influenced her management of the Meganet contract as well as her favorable assessment of Meganet's capabilities, cited by the OIG audit in Finding 3 (pp. 16, 20). The Office of the Solicitor discusses how to avoid conflicts of interest in its required annual ethics seminars. To effectuate the OIG's recommendations with

regard to conflicts and reporting obligations, the Office of the Solicitor will continue to address both subjects in its 2005 ethics training, and appropriate reminders will be sent to employees.

Based upon the extensive documentation provided by OASAM to the OIG in response to its audit, it appears that Recommendations 4, 6 and 8 already have been substantially addressed. In fact, the Department made significant changes to its procurement policies in 2003, in direct response to the Meganet contract problems which the ASAM uncovered and referred to the OIG. Specifically, the Department prohibited any expenditures for sole-source contracts exceeding 10 percent of the amount approved by the Procurement Review Board, and the contract duration approved by the Board, without prior approval from the Department's Chief Acquisition Officer. Further, the Department's information technology (IT) governance structure, which includes the Technical Review Board, limits purchases of IT products prior to obtaining documentation that the products are deployable in the Department's system environment. The Department also has reinforced its policy requiring that pre-award activities are completed and documented prior to execution of any final procurement contract.

In addition, the OIG report reveals that the acts and omissions of certain IT staff contributed to the procurement problems discovered by the ASAM and confirmed by the OIG. It is important to note that OASAM has made significant changes among the staff closest to the award of the encryption contracts audited by the OIG. The former Deputy CIO left the Department in April 2003 and subsequently separated from Federal service altogether. She was replaced by a highly experienced IT professional with substantial knowledge of contracts administration, who has instituted a number of management, training and accountability measures to strengthen the Department's IT acquisition process.

The senior procurement official with responsibility for the software acquisition process audited by the OIG also was replaced. This individual was reassigned by OASAM management a year ago, and a new, experienced contracting professional was hired in August 2004. Both of these highly qualified replacements came from outside the Department of Labor. The Department also has replaced other IT staff who worked closely with the former Deputy CIO. These personnel changes, together with the procedural protections instituted after the Meganet contract, should help prevent such procurement problems in the future.

The OIG's report strongly (and justifiably) criticizes the Department's award of an encryption software contract to Meganet (e.g., "Therefore, there is no assurance that Meganet actually was the only (or best) small business capable of meeting ITC's file encryption requirement." *OIG audit report*, p. 5). On the other hand, the report also questions the Department's decision to set aside the Meganet contract and appears to explicitly endorse Meganet's technical capabilities – relying heavily on representations made by the former Deputy CIO and top Meganet officials.

For example, on p. 17 the report notes, "According to Meganet's Corporate Counsel, Meganet staff successfully responded to all operational concerns raised by DOL at these meetings." It is my understanding that the "Corporate Counsel" cited here is the same individual with whom the Deputy CIO is reported by the OIG to have had an apparent conflict of interest. The report also attaches weight to the fact that "the former Deputy CIO had, prior to her departure from DOL in March 2003, argued that the Meganet products worked and could be implemented." (p. 20) And

***Award and Management of Contracts for
Encryption Software Were Significantly Flawed***

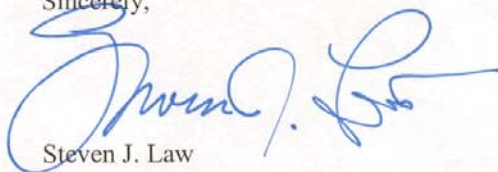
the report states that OIG technical staff “was able to demonstrate the functionality of Meganet’s VME Office 2003 product,” in a controlled test involving three computers that was “assisted by Meganet personnel.” (p. 20)

Based on these views and the Meganet-assisted product demonstration, the report recommends that the Department’s Information Technology Center be directed to conduct a formal test of Meganet products to determine their usefulness in meeting the Department’s encryption needs (*OIG Audit Report Recommendation 7*).

This presumes, however, that even a successful test would enable the Department to deploy the Meganet product effectively. According to Office of Management and Budget (OMB) guidance on PKI as of December 20, 2004 (*See Memorandum M-05-05, “Electronic Signatures: How to Mitigate the Risk of Commercial Managed Services”*), all Federal agencies are required to use one of three OMB approved shared-service providers for PKI services. None of the three OMB-approved PKI service providers utilize Meganet encryption software. Moreover, Meganet has encountered protracted delays in gaining the required security certification for any cryptographic product before it can be deployed on a Federal technology system. In fact, not until January 27, 2005 did Meganet receive the required NIST certification for its encryption software – 3 years after DOL entered into a contract with the company. Considering the change in government-wide direction for the implementation of PKI, and the long-delayed certification of the Meganet encryption software, it is doubtful that the Labor Department could realize significant value from Meganet’s product in the long term, regardless of the results of further testing. By contrast, the Entrust encryption product has been NIST-certified since 1999, and is used by two out of the three shared-service providers for PKI services approved by OMB.

I would like to commend your staff for assembling a thorough report that confirms our concerns about this matter and offers constructive recommendations to prevent contracting problems in the future. We will continue to assess our progress – and take appropriate actions – to enhance the procedural and personnel changes that have already been instituted by the Department since the events that gave rise to the OIG’s audit.

Sincerely,



Steven J. Law