U.S. DEPARTMENT OF COMMERCE
Office of Inspector General

OFFICE OF THE SECRETARY

Information Security in Information Technology Service Contracts Is Improving, But Additional Efforts Are Needed

Final Inspection Report No. OSE-16513/September 2004

PUBLIC RELEASE

Office of Systems Evaluation

UNITED STATES DEPARTMENT OF COMMERCE
The Inspector General
Washington, D.C. 20230

SEP 29 2004

MEMORANDUM FOR: Otto Wolff
Chief Financial Officer and
Assistant Secretary for Administration

Thomas N. Pyke, Jr.
Chief Information Officer

FROM: Johnnie E. Frazier

SUBJECT: *Information Security in Information Technology Service Contracts Is Improving, but Additional Efforts Are Needed*
Final Inspection Report No. OSE-16513

In September 2003, we reported the results of our independent evaluation of the Department of Commerce's information security program and practices for unclassified systems, as required by the Federal Information Security Management Act (FISMA).[1] As part of our evaluation, and in accordance with guidance provided by the Office of Management and Budget (OMB),[2] we assessed the Department's progress in ensuring that information security is being adequately addressed in information technology (IT) service contracts in light of our May 2002 report on the weaknesses we identified in a sample of 40 such contracts.[3]

As you will recall, we found that most of the 40 contracts had either insufficient security provisions or none at all. We concluded that federal and departmental policy and guidance for incorporating such provisions were lacking and made recommendations for addressing this area.[4] The following table provides a summary of the recommendations presented in the May 2002 report and the status of the actions taken to address them as reported by the Department.

---

[1] U.S. Department of Commerce Office of Inspector General, September 2003. *Independent Evaluation of the Department of Commerce's Information Security Program Under the Federal Information Security Management Act,* OSE-16146. Washington, D.C.: Department of Commerce OIG.

[2] Memorandum for Heads Of Executive Departments and Agencies, Joshua B. Bolten, Director, Office of Management and Budget, "Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security," August 6, 2003.

[3] U.S. Department of Commerce Office of Inspector General, May 2002. *Information Security Requirements Need to Be Included in the Department's Information Technology Service Contracts,* OSE-14788. Washington, D.C.: Department of Commerce OIG.

[4] A summary of our recommendations and their status is attached.

OFFICE OF INSPECTOR GENERAL
OIG
U.S. DEPARTMENT OF COMMERCE

SUMMARY OF OIG RECOMMENDATIONS AND STATUS OF DEPARTMENTAL ACTIONS

RECOMMENDATION	ACTIONS TAKEN (As Reported By The Department)
1. The Procurement Executive, with the Chief Information Officer (CIO), should develop and disseminate a comprehensive policy for acquisitions of IT systems and services.	a. Procurement memorandum (PM) issued on 09/13/00 reemphasized importance of security. PM provided list of resources to assist contract staff. b. CIO issued IT Security Program and Policy. This policy was added to the resource list identified in the PM.
2. The Procurement Executive, with the CIO and advice of the Office of General Counsel (OGC), should establish standard contract provisions for safeguarding the security of unclassified systems and information and include such provisions in solicitations and contracts for IT services.	a. In 06/03, draft provisions were provided to the Commerce acquisition community, OCIO, OGC, and OIG for comment, and a meeting was held to resolve issues. b. Clauses were issued in final 11/17/03. Clauses became mandatory for new solicitations and contracts for services on 01/01/04. Existing service contracts were to be modified as appropriate by 03/01/04.
3. The Procurement Executive, with program officials and OGC advice, should instruct all heads of contracting offices to review current solicitations and contract actions to determine whether modification is needed to include security provisions.	a. The Office of Acquisition Management (OAM) completed an assessment, and a list of contract actions needing modification to incorporate new security clauses was generated for each contracting office within the Department. This list was forwarded for action by the contracting offices at the end of 01/04.
4. The Procurement Executive, with the CIO and program officials, should ensure that contracting officers, contracting officer's technical representatives (COTRs), and other procurement personnel have job-specific information security training.	a. All Department and contract employees completed basic security awareness training. b. Content of job-specific security training module for acquisition staff (including COTR) finalized in 08/03. Implementation is pending.
5. The Procurement Executive, with the CIO and program officials, should ensure that contracting officers, IT staff, and program officials are aware of and use NIST Special Publication 800-4, *"Computer Security Considerations in Federal Procurements"* (Note: As of October 2003, NIST Special Publication 800-64 ,*"Security Considerations in the Information System Development Life Cycle,"* has superceded NIST Special Publication 800-4.*)*	a. Procurement memorandum issued on 09/13/00 reemphasized the importance of security. PM provided list of resources to assist contract staff, which includes NIST Special Publication 800-4.

To assess the Department's progress in fiscal year 2003, we reviewed its new security policy and a sample of IT service contract actions issued as of October 1, 2002. The findings from this review were summarized in our September 2003 FISMA report. We found that the Department's newly issued information security policy contains appropriate requirements for contractors and other government agencies that support Commerce. The Department also drafted standard contract provisions for safeguarding the security of sensitive but unclassified systems and information, which require, among other things, a certification and accreditation package.[5,6] for contracted IT resources/services that involve connection to Commerce networks or storage of Commerce data on contractor-owned systems.[7] However, while most of the contract actions we reviewed contained some security coverage, adequate provisions for controlling access to departmental systems and networks were still missing. We also found little coordination among the contracting, technical, and security staff responsible for developing contract-specific security requirements and minimal oversight of individual contractor compliance with security requirements.

Although our findings were presented in our September 2003 FISMA report, we did not make recommendations. This memorandum report provides additional discussion of these findings as well as recommendations to further ensure that information and information systems are adequately secure when contractor-provided services are used.

Discussion of Department's Response to the Draft Report

In a July 12, 2004 memorandum, the Chief Financial Officer and Assistant Secretary for Administration agreed with our three recommendations and described corrective actions that are planned or under way. His subsequent September 28, 2004, memorandum provided additional information on the corrective actions. We concur with the actions described, which are summarized below. The complete response is included as an attachment to this report.

In response to our first recommendation to review a sample of current IT service contracts to determine whether they have been modified where necessary to incorporate appropriate security provisions, the response states that the Procurement Executive will ask each Department contracting office to detail the status of efforts to incorporate security provisions into current contracts and require offices that have not completed the effort to set milestones for doing so. The response also states that the Procurement Executive's staff is currently working with the Department's CIO Office to incorporate a review of service contracts in the FY 2004 IT security compliance review program. It indicates that a random sample of contracts will be reviewed to determine whether or not contracting offices have modified applicable contracts to include the mandatory IT security contract clauses.

---

[5]Certification is the formal testing of the security safeguards implemented in a computer system to determine whether they meet applicable requirements and specifications. Accreditation is the formal authorization by management for system operation, including an explicit acceptance of residual risk.

[6]Documentation required in the certification and accreditation package includes a system security plan, other system information (e.g., risk assessment, contingency plans, information on security training, security roles and responsibilities, and system documentation), and certification documentation (i.e., test plan and test results) and the certifier's recommendation

[7] At the time of our fiscal year 2003 FISMA report, the contract provision was under departmental review. It was finalized in November 2003.

Our second recommendation is to implement procedures to strengthen communication between the contracting officer, COTRs, and information security staff. The response states that the Procurement Executive will work with the CIO's office and program officials to strengthen communicationand put controls in place that use existing contract management, review, and compliance processes to ensure that IT security is considered during the pre-solicitation, award, and post award phases of the acquisition process. It also indicates that the Procurement Executive's staff will issue guidance on IT security contract requirements throughout the various phases of the acquisition process and incorporate training on these requirements into the CO/COTR IT security training module that is currently being developed.

Our third recommendation is to establish procedures and accountability for reviews of contractor compliance with security procedures and controls. The response states that the Procurement Executive, CIO, and OGC staffs will work together to ensure adequate reviews are incorporated into existing contract review processes and coordinated among the CO, COTR, system owner, and information security staff; and that the Procurement Executive staff will issue guidance regarding these reviews.

We appreciate the cooperation and courtesies extended to us by the Office of Acquisition Management, the Office of the Chief Information Officer, and the contracting offices at the bureaus we reviewed.

BACKGROUND

The Department continues to rely heavily on contractors to provide IT services. In fiscal year 2003, $350 million of the nearly $535 million Commerce spent on IT contracts went to contractors for services, such as software development, installation, configuration, testing, operations, and maintenance, as well as website development and management.

Federal regulations and departmental guidance require that individuals, including contractors, who have access to information systems follow established security rules and be held accountable for safeguarding systems and data. To hold contractors accountable, contract solicitations and award documents should include appropriate security provisions. In addition, appropriate contract administration procedures such as performance measurement and onsite inspections should be in place to ensure that contractors are using appropriate methods for safeguarding the Department's sensitive information systems and data. Compliance reviews should be consistent with agency policies for testing and evaluating information security policies and controls.

OBJECTIVES, SCOPE, AND METHODOLOGY

Our purpose was to expand upon our 2003 FISMA findings and provide additional recommendations based on our follow-up review of the Department's progress in implementing the recommendations in our May 2002 report. As part of this process, we reviewed current departmental and acquisition policies, and examined a sample of 24 contract actions awarded from October 1, 2002, through July 31, 2003, by a cross-section of departmental units.[8] We reviewed contract documentation to determine whether adequate security provisions were included and if so, whether contractors were complying with the requirements. Our scope was limited to contracts dealing with sensitive but unclassified systems and information.

The Department Needs to Ensure that IT Service Contracts Contain the New Security Clauses and that Appropriate Contract Oversight Occurs

The Department has made significant progress in implementing our previous recommendations. A new information security program policy was issued in January 2003, which states that IT security officers, systems owners,[9] and COTRs must work together to ensure that information security is adequately addressed throughout the acquisition process. It also states that contracts must include language requiring contractors and subcontractors to give the Department access to facilities, operations, documentation, databases, and personnel used in performing the contract, for the purpose of ensuring contractor compliance in safeguarding government information and systems. In an April 2003 policy memorandum, the Office of Acquisition Management (OAM) reemphasized the importance of considering IT security in acquisitions, and recommended the new information security policy be used as an additional resource in addressing IT security issues. According to the Department, all employees have completed security awareness training, and the content of an IT security training module for the acquisition community (including COTRs) has been approved, and implementation is pending.

Additionally, OAM, with the assistance of the Department CIO's office and program officials, drafted two comprehensive standard contract clauses for safeguarding unclassified systems and information. These are to be included in all solicitations and contracts for services that involve IT or require contractor access to information systems and/or data. The first—Commerce Acquisition Regulation (CAR) 1352.239-73, *Security Requirement for Information Technology Services*—requires contractors (and subcontractors) and their employees to adhere to specific information security policy, and holds them to the standards of accountability for sensitive federal information systems and data that apply to federal employees. When contractor-owned systems are to be interconnected with a departmental system or process and/or store government data, the clause requires the contractor to provide, implement, and maintain an IT security plan, and submit a system certification and accreditation package. The second clause—CAR 1352.239-74, *Security Processing Requirements for Contractors/Subcontractors Personnel for Accessing DOC Information Technology Systems*—requires any contractor personnel needing

[6] The Department's Office of the Secretary, the National Oceanic and Atmospheric Administration, the National Institute of Standards and Technology, the Bureau of the Census, and the U.S. Patent and Trademark Office

[7] The Department's information security policy defines a system owner as a project manager with day-to-day management and operational control over the system and direct oversight of the system/network administrators and operations staff.

access to departmental systems (1) be appropriately screened according to the risk level of the work being performed, and (2) complete security awareness training. This clause also requires inclusion of CAR 1352.209-72, *Restrictions Against Disclosures*, an existing clause that requires contractors to agree to keep government furnished information in the strictest confidence and to restrict access to such information on a need-to-know basis. The two new clauses were finalized in November 2003 and became mandatory for all new solicitations and contracts for services on January 1, 2004. Existing contracts were to be modified to include the clauses, as appropriate, by March 1, 2004.

Review of Contracts Needed to Ensure Appropriate Inclusion of New Clauses

Though the standard clauses had not been finalized at the time of our FY 2003 FISMA review, the Department's information security policy and acquisition guidance emphasized the need for IT security provisions in contracts. Most contract actions we assessed for the FY 2003 review contained at least minimal provisions, primarily related to personnel security, i.e., requirements for risk and suitability assessments and background clearances for contractors working in government facilities; some included requirements for contractors to attend security awareness training and follow departmental and/or bureau information security procedures. However, only 2 of the 24 contracts we reviewed contained comprehensive security provisions like those that were being developed by the Department, which require contractors to adhere to specific IT security policy and to be accountable for federal information and information systems.

When the standard contract provisions for safeguarding unclassified systems and information became mandatory, OAM provided a list of current contract actions to heads of contracting offices (HCOs) and asked them to review the list, determine which actions might need the new clauses, modify them accordingly by March 1, 2004, and notify the Department's Procurement Executive if the deadline could not be met. These are important steps. However, to ensure the Department's sensitive information and information systems are protected, OAM now needs to take the additional step of periodic reviewing a sample of contracts in each operating unit to confirm inclusion of the appropriate security provisions.

Contractors' Compliance With Information Security Provisions Needs Oversight

We found little evidence of appropriate review of contractor compliance with security requirements. FISMA requires that controls be in place to protect the government's information and information systems and that these controls be periodically tested and evaluated. OMB's reporting instructions to agencies and inspectors general ask whether appropriate methods have been used to ensure that contractor-provided services comply with security guidelines. The Department's information security policy requires that contractors adhere to the Department's established security policies when working with Commerce IT systems and data, and as previously stated, that contracts contain provisions allowing access for the purpose of IT inspection, investigation, and audit.

The Department's fiscal year 2003 FISMA report indicated that appropriate methods were used to ensure that contractor-provided services comply with security guidelines, but cited only one specific compliance mechanism—an automated notification system informing COTRs of

contractors who fail to complete security awareness refresher training within the required time frame. Contracting staff we spoke with were not aware of any compliance inspections of contractors' facilities or operations, nor was there any evidence in the contract files to indicate such reviews had been performed. These inspections are not solely the responsibility of the contracting office; there needs to be coordination among COTRs, departmental systems owners (or cognizant program officials), and security officials to determine and implement an appropriate review strategy.

Conclusion

With the contract clauses finalized and their use mandated, the Department has a solid foundation for improving security in its IT service contracts. The clauses are comprehensive enough to ensure that contractors and their employees are aware of their duties and responsibilities for adequately safeguarding sensitive data and systems. Contracting officers, COTRs, systems owners, and IT security staff must work together to include any additional requirements specific to the systems and data being accessed by contractor employees, and continue to monitor and identify any security issues throughout the life cycle of the contract. The implementation of the IT security training for COs and COTRs will also foster awareness.

Contracting, technical, and program personnel, as well as IT security staff have a significant management and oversight role in ensuring that adequate controls are in place and contractors are adhering to the appropriate information security policies. The Department needs to strengthen communication among these personnel in ways that will foster consistent integration of adequate security in IT service contracts.

Mechanisms for strengthening this communication could include (1) requiring the IT security staff to sign off on the procurement request; (2) having IT security staff and the COTR complete an information security checklist in the preaward phase for inclusion in the contract file so that information security is considered during requirements definition and solicitation; and (3) throughout the contract's performance period, holding regularly scheduled information security status meetings among the contracting officer, COTR, system owner, and information security staff to discuss contractor performance.

Moreover, to ensure contractor compliance with security procedures and controls, the Department's Procurement Executive, with assistance from the CIO, needs to establish procedures and assign accountability for conducting reviews of service contracts, in accordance with FISMA, OMB policy, NIST guidance, and the Department's information security policy, to ensure that contractors are complying with security procedures and controls. Criteria should be established, including the scope, nature and frequency of the reviews. These reviews should be coordinated among the contracting officer the COTR, the system owner, and the information security staff, with documentation of the review included in the contract file.

RECOMMENDATIONS

The Chief Financial Officer and Assistant Secretary for Administration should take the necessary steps to ensure that the Department's Procurement Executive, with the CIO's assistance, does the following:

1. Reviews a sample of current contracts to determine whether appropriate security provisions have been incorporated.

2. Implements procedures to strengthen communication between the contracting officer, COTRs, and information security staff.

3. Establishes procedures and assigns accountability to the CO and COTR, as appropriate, to conduct reviews of service contracts, in accordance with FISMA, OMB policy, NIST guidance, and the Department's information security policy, that will ensure contractor compliance with security procedures and controls.

    a. Criteria should be established, including the scope, nature and frequency of the reviews.
    b. These reviews should be coordinated among the contracting officer, the COTR, the system owner, and the information security staff.
    c. Documentation of the review should be included in the contract file.

Attachment

cc: Michael S. Sade, Director for Acquisition Management and Procurement Executive, U.S. Department of Commerce
Karen Hogan, Deputy Chief Information Officer, U.S. Department of Commerce
William Lay, Director, IT Security, Infrastructure, and Technology, U.S. Department of Commerce

ATTACHMENT

UNITED STATES DEPARTMENT OF COMMERCE
Chief Financial Officer
Assistant Secretary for Administration
Washington, D.C. 20230

JUL 12 2004

MEMORANDUM FOR: Judith J. Gordon
Assistant Inspector General for Systems Evaluation
Office of Inspector General

FROM: Otto J. Wolff
Chief Financial Officer and
Assistant Secretary for Administration

SUBJECT: *Information Security in Information Technology Service Contracts is Improving, but Additional Efforts are Needed* – Draft Inspection Report No. OSE-16513

This memorandum provides our response to the findings and recommendations in your draft report, on information security in the Department of Commerce's information technology service contracts.

In general, we agree with the findings and conclusions found in the subject draft report. We will continue to work on the specific details (milestones, implementation plans, etc.) to address those concerns and specific recommendations set forth in the draft report, as well as the final report. Our comments address each of the three recommendations made in the draft report.

Recommendation #1 – Review a sample of current contracts to determine whether appropriate security provisions have been incorporated.

We agree with the recommendation that the Department's Procurement Executive should determine whether appropriate security provisions have been incorporated into current contracts as required by Procurement Memorandum 2003-09, Information Technology Security Clauses, issued November 17, 2003. To accomplish this, the Department's Procurement Executive staff will request the status of incorporation of the required clauses in applicable contracts from each Department contracting office. In those instances where the clauses have not been incorporated, the Procurement Executive will require that the contracting office provide established milestones for incorporation. Procurement Executive staff will monitor to ensure the established milestones for incorporation are met. The request for status is anticipated to be completed by July 31, 2004.

Recommendation #2 – Implement procedures to strengthen communication between the contracting officer, COTRs, and information security staff.

We agree that communication between the contracting officer, Contracting Officer Technical Representatives (COTR), and information security staff should continue to be strengthened. The Procurement Executive strongly supports communication and partnership within the acquisition community (Contract Specialists, Contracting Officers and Contracting Officer Technical Representatives (COTR)/Contracting Officer Representatives (COR)), with stakeholders such as the Office of Chief Information Officer (OCIO), Office of Inspector General (OIG), Office of General Counsel (OGC), as well as with program officials. The recently issued Commerce Acquisition Manual (CAM) Chapter 1301.670, Contracting Officer Representative Certification Policy, emphasizes the importance of communication by stating that the purpose of the program is to "...create a results oriented acquisition workforce focused on partnering, performance, quality, and accountability that ensures entrusted resources are used and managed wisely throughout all phases of the acquisition lifecycle." The COR Program incorporates the development of skill based competencies such as General Management Knowledge and Performance, and Procurement Knowledge and Performance. The development of the competencies include the demonstration of skills such as the ability to partner, communicate and team, as well as an understanding and application of the COTR/CORs role in the procurement process, and how the CO and COTR/COR must work together with their stakeholders throughout the acquisition life cycle to ensure success. The Procurement Executive will continue to foster communication and partnering beginning at the highest levels within the Department and will continue to develop acquisition policies that incorporate the concepts of teaming, partnership and communication.

Recommendation #3 – Establish procedures and assign accountability to the CO and COTR, as appropriate, to conduct reviews of service contracts, in accordance with FISMA, OMB policy, NIST guidance, and the Department's information security policy, that will ensure contractor compliance with security procedures and controls.

We concur with the recommendation. The Department's Procurement Executive, in coordination with the OCIO and program officials, will work to ensure that adequate reviews are performed at the appropriate levels in accordance with the Federal Information Security Management Act (FISMA), Office of Management and Budget (OMB) policy, National Institute of Standards and Technology (NIST) guidance and the Department's information security policy to ensure contractor compliance with security procedures and controls. Procurement Executive staff will collaborate with the OCIO and OGC to ensure that adequate reviews are incorporated into the existing contract review process and that the reviews are coordinated among the CO, COTR/COR, the system owner and the information security staff. The Procurement Executive staff will ensure that guidance is issued to ensure proper documentation of such reviews is included in the contract file. The Procurement Executive will issue guidance that reinforces the

existing requirement of the CO and COTR to monitor contract performance. The guidance will require that COs and COTRs ensure that contractor compliance with security procedures and controls are incorporated into already existing performance management processes. The Procurement Executive staff will also collaborate with the OCIO to evaluate the possibility of integrating contract reviews into the information security annual Compliance Review Program. The issuance of guidance by the Procurement Executive is anticipated to be completed by September 30, 2004.

We appreciate the opportunity to comment on the draft report, and we look forward to receiving a copy of the final report. If you have questions or would like to discuss the responses in this memorandum, please contact Michael S. Sade at (202) 482-4248.

UNITED STATES DEPARTMENT OF COMMERCE
Chief Financial Officer and
Assistant Secretary for Administration
Washington, D.C. 20230

SEP 28 2004

MEMORANDUM FOR: Judith J. Gordon
Assistant Inspector General for Systems Evaluation
Office of Inspector General

FROM: Otto J. Wolff
Chief Financial Officer and
Assistant Secretary for Administration

SUBJECT: *Information Security in Information Technology Service Contracts is Improving, but Additional Efforts are Needed*
- Draft Inspection Report No. OSE-16513

This memorandum supplements our July 12, 2004 response to the findings and recommendations in your draft report, on information security in the Department of Commerce's (DOC) information technology (IT) service contracts. Specifically this memorandum provides additional information to support our response to *Recommendation No.2 - Implement procedures to strengthen communication between the Contracting Officer (CO), Contracting Officer Technical Representative (COTR), and Information Security staff.*

We concur with the recommendation. The Department's Procurement Executive, in coordination with the Office of the Chief Information Officer (OCIO) and program officials, will work to ensure that communication is strengthened and that adequate controls are in place to ensure that IT Security is considered during the pre-solicitation, award and post award phases of the acquisition process. Procurement Executive staff will collaborate with the OCIO and the Office of General Counsel (OGC) to ensure that IT Security contract requirements are adequately incorporated into existing contract review processes, the IT Security Compliance Review Program, and existing contract compliance and management processes. The Procurement Executive staff is currently working with the OCIO to incorporate a review of service contracts in the FY 04 IT Security Compliance Review Program. A random sample of contracts will be reviewed to determine whether or not Contracting Offices have modified applicable contracts to include the mandatory IT Security contract clauses. The Procurement Executive and the OCIO will continue to work together to determine additional ways to partner to address the IT Security recommendations of the Office of Inspector General.

The Procurement Executive staff will issue guidance that outlines the IT Security contract requirements throughout the various phases of the acquisition process and will ensure that such requirements are incorporated into the CO/COTR IT Security Training module that

is currently being developed. Substantial coordination with the OCIO, the OGC and the DOC Acquisition Offices will be required to complete Recommendation No. 2. It is anticipated that guidance will be issued by March 31, 2005.

We appreciate the opportunity to supplement our July 12, 2004 response to the draft report, and we look forward to receiving a copy of the final report. If you have questions or would like to discuss the responses in this memorandum, please contact Michael S. Sade at (202) 482-4248.