U.S. DEPARTMENT OF COMMERCE
Office of Inspector General

OFFICE OF THE SECRETARY

Information Security Requirements Need To be Included in the Department's Information Technology Service Contracts

Final Inspection Report No. OSE-14788/May 2002

PUBLIC RELEASE

Office of Systems Evaluation

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

MAY 15 2002

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

FROM: Johnnie Frazier

SUBJECT: *Information Security Requirements Need to Be Included in the Department's Information Technology Service Contracts*
Final Inspection Report No. OSE-14788

This is the final report on our review of information security provisions in the Department of Commerce's information technology service contracts.

In September 2001, we completed an independent evaluation of the Department's information security program, as required by the Government Information Security Reform Act. We issued a report[1] that identified numerous information security weaknesses throughout the Department, including the lack of sufficient policy and guidance to ensure that contract documents for IT services contain adequate information security provisions.

Our report discusses this weakness further and makes recommendations to correct it. These recommendations are based on the results of our review of a sample of the Department's IT service contracts, which revealed that security provisions to ensure the safeguarding of sensitive but unclassified systems and information are either missing or inadequate. In the written response to our draft report, you agreed with all of our recommendations and described corrective actions being taken or planned. Where appropriate, we have included a synopsis of the response and our comments. The complete response is included as an attachment to this report.

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

[1] *Independent Evaluation of the Department's Information Security Program*, Inspection Report No. OSE-14384, September 2001.

INTRODUCTION

The Government Information Security Reform Act (GISRA) addresses the federal government's need to manage, implement, oversee, and ensure the security of unclassified and national security information systems. It requires that agencies conduct annual reviews of their information security programs and that the Office of Inspector General for each agency conduct separate, independent evaluations of these programs to determine whether they comply with GISRA.

OMB's reporting instructions for GISRA reviews stipulate that these evaluations should assess an agency's specific methods for ensuring that contractor-provided IT services are sufficiently secure and meet the requirements of GISRA, OMB policy, and other computer security guidance and policy. To address this particular instruction, we reviewed a sample of IT service contracts[2] issued by the Department. We found that information security provisions in these contracts are inadequate, primarily because of a lack of specific federal and departmental guidance on safeguarding sensitive information in federal procurements.

We noted this finding in our September 2001 evaluation report, which was submitted to OMB. In response, OMB requested a briefing on our concerns about the lack of specific federal guidance, which we provided on January 14, 2002. OMB officials told us that they share our concerns and plan to address the weaknesses in federal policy and guidance through a working group being established to support implementation of Executive Order 13010, *Critical Infrastructure Protection in the Information Age*. In the meantime, we believe the Department should take steps, as outlined in this report, to safeguard its sensitive information assets in contracts for IT services.

BACKGROUND

As the federal workplace has become more dependent on information technology, the federal government has increasingly relied on outside contractors to perform various IT services, including software development, installation, configuration management, testing, operations, and maintenance. Other commonly outsourced IT functions include web site development and maintenance and database management. These services may be performed onsite or by remote access from contractors' facilities. In many cases, contractors have access to sensitive information, or, by virtue of the services they perform, may be able to gain access to such information.

According to the Clinger-Cohen Act, IT includes not only computers, software, and ancillary devices, but also related services. OMB Circular A-130, Appendix III, *Security of Federal Automated Information Systems,* requires all individuals with access to systems to follow the security rules established for those systems. Thus, contractors performing IT services for the government should be held to the same standards of accountability as government personnel for maintaining the security of systems, networks, and the information contained therein.

[2] The word "contracts" as used here includes other procurement actions, for example, modifications and task orders to contracts, delivery orders under multiple award schedule contracts and governmentwide agency contracts, and purchase orders.

Inadequate Information Security Provisions Can Result in Security Violations

Inadequate information security provisions in IT service contracts can reduce the government's ability to oversee and monitor the contract and to hold the contractor accountable for providing information security. Inadequate requirements may also result in a loss of privacy or in security violations. For example, when remote access is required, confidentiality and integrity of data may suffer if the contractor's method of remote access is not secure. Inadequate controls over access to systems can lead to unauthorized access to and modification or destruction of systems and data by contractor personnel or intruders.[3]

OBJECTIVES, SCOPE, AND METHODOLOGY

The objective of our review was to determine whether adequate information security provisions are included in contracts for information technology services. We selected a random sample of 40 contract actions for IT services awarded by departmental contracting offices[4] for the period October 1, 1998, through July 31, 2001. We reviewed contract documentation to determine whether systems and information security was considered during the procurement process and whether adequate information security provisions were included in the contract. We also reviewed federal and departmental acquisition and IT policies, held discussions with contracting officers within the Department, and obtained information on security practices and guidance both from other federal agencies and from Carnegie Mellon University's Software Engineering Institute. Our scope was limited to contracts dealing with sensitive but unclassified systems and information.

We performed our work in accordance with the Inspector General Act of 1978, as amended, and the *Quality Standards for Inspections*, March 1993, issued by the President's Council on Integrity and Efficiency.

FINDING

IT Service Contracts Frequently Lack Adequate Information Security Provisions

Our review of contract actions for information technology services revealed that information security provisions were either totally missing or inadequate. Forty-one percent of the actions reviewed contained no such provisions. The other 59 percent contained minimal coverage, typically dealing with contractor employee screenings, facilities access, and privacy. However, none of these contained adequate provisions to safeguard the Department's computer systems and networks from unauthorized access and its data from unauthorized disclosure or modification.[5] Fewer than 1 percent of the actions reviewed contained evidence that information security was considered during

[3] *Security for Information Technology Service Contracts*, Software Engineering Institute, Carnegie Mellon University, Report No. CMU/SEI-SIM-003, January 1998.
[4] The contracting offices included in our review are located within the Office of the Secretary, the U.S. Patent and Trademark Office, the National Oceanic and Atmospheric Administration, the Bureau of the Census, and the National Institute of Standards and Technology.
[5] Most of the U.S. Patent and Trademark Office contract actions contained clauses safeguarding patent data, and a few of the Bureau of Census actions discussed nondisclosure of Title 13 data.

the acquisition planning process. Based on the results of this sample, it is likely that the majority of IT service contracts throughout the Department lack needed information security provisions. To remedy this problem, IT service contracts and solicitations should be reviewed and, as necessary, revised to include needed security provisions.

Contract Information Security Requirements and Oversight Should Be Expanded

The most frequently included information security provisions in IT service contracts are for contractor employee background screenings, facilities access, and Privacy Act compliance. However, adequate protection of the Department's sensitive systems and information also requires safeguards associated with the specific network and computing technologies to be used, the nature of the work to be performed, the method of access to departmental systems and networks, and the installation of software.

Contractors must be required to follow the pertinent information security policies of the agency, such as for privacy, access, and authentication. They should also be required to limit the government's vulnerability to known forms of attack for the specific technologies being used. If contractor software is to be installed and operated on departmental systems, contracts must contain provisions to ensure that the software will not harm the system or introduce vulnerabilities. When remote access is needed, policies and procedures for secure communications must be established and enforced to prevent intrusions, interception of data, or denial of service. Contractor access to agency systems should be strictly controlled by scheduling access in advance to the extent possible, limiting access only to resources essential to performing the work, and revoking access in a timely manner when it is no longer needed.

Department contracting, technical, and programmatic personnel have considerable management and oversight responsibilities in the area of government IT security. They must ensure that the selected contractor has the capability to meet the information security requirements and is committed to doing so by the terms and conditions of the contract. They must also ensure that contractor software has been installed correctly and is checked periodically to determine if it has been changed. Relevant directories and files must be examined periodically to detect unexpected changes, which may indicate that an intrusion has occurred, and system and network logs should be regularly inspected for evidence of unexpected activity. A process must be established for reviewing, on a regular basis, the contractor's compliance with the security requirements and for implementing corrective actions if problems are found, including possible renegotiation of the contract.

The foregoing discussion is illustrative and does not cover all considerations. Contract requirements and departmental oversight must be tailored to the specific risks and issues associated with the contract. More detailed considerations and guidance are presented in the Appendix to this report. Clearly, contracting officers will need support from information security experts in chief information officer organizations and operating unit program officials to ensure that adequate information security provisions are included and enforced in contracts.

Specific Guidance for Contracting Officers is Minimal and Unclear

The lack of adequate contract requirements for information security is attributable in large measure to the lack of specific federal and agency guidance on this subject. At present, the Federal Acquisition Regulation (FAR) and Commerce policies do not provide contracting officers with the information they need to effectively deal with this complex area.

Current IT security regulations and policy include contractor-provided services in their coverage, but guidance provided to contracting officers on how to incorporate information security provisions in federal contracts is minimal and unclear. FAR Part 39, "Acquisition of Information Technology," states that acquisition of IT must be consistent with OMB Circular A-130, but contains no specific information on what needs to be done. FAR Part 39.105 addresses Privacy Act protection in contracts for commercial IT services or IT support services, stating that contracts pertaining to a system of records[6] must include specific safeguards. The FAR defines a "record" as information about an *individual* that is maintained by an agency. In our discussions with some Commerce contracting officers and their legal counsel, we learned that they interpret this clause as applicable only to acquisitions in which information about individuals will be accessed, and they therefore do not require the safeguards discussed in it on other types of contracts. To ensure across-the-board protection of the Department's sensitive but unclassified systems, standard contract provisions are needed in solicitations and contracts for safeguarding the security of unclassified systems and information.

Policies for safeguarding sensitive systems and data are contained in the Department's *IT Security Handbook*. These policies apply to all IT resources, including those being developed or accessed by contractors. According to the policy, all Commerce organizations must maintain an information security program, and documents for acquiring IT or IT services must contain appropriate information security requirements. However, because the handbook lacks guidance as to what specifically should be done to ensure information security in contracts, the policy generally has not been implemented in the Department's contracts.

Commerce Acquisition Manual Notice 00-02, *Security Processing Requirements for On-Site Service Contracts*, dated April 18, 2000, addresses unclassified service contracts performed in government facilities. Although it requires a risk assessment, the manual deals primarily with the need to obtain background checks on contractor employees. In response to our September 2001 GISRA evaluation report, the Department's Office of Acquisition Management issued Procurement Memorandum 2001-02, *Importance of Information Technology Security to Acquisition.* Despite the fact that it stresses the importance of protecting information security throughout the acquisition process and working with the CIO's office, the memorandum contains no specific guidance, such as that shown in the Appendix, as to how that goal can be accomplished.

The Computer Security Act and GISRA give NIST the responsibility for issuing policy related to computer security. NIST Special Publication 800-4, *Computer Security Considerations in Federal Procurements,* contains detailed information on protecting information security throughout all phases of IT acquisitions. Although it is very informative and contains much useful information

[6] See FAR Part 24.101.

related to information security, this document was written in 1992, prior to the enactment of significant changes in procurement law and related acquisition reforms, and parts of it have become outdated. In addition, the contracting officers we spoke with were not aware of its existence. According to NIST, the document is currently being updated, with completion scheduled for the end of the fiscal year. Until the update is completed, contracting officers should be reminded to use this document, as it still remains a valuable tool.

Information Security Training Should Be Included in Career Development Training for Contracting Staff

Providing guidance to contracting staff will not be enough: they must also receive training to understand how to apply the guidance. According to the Department's CIO office, information security training is the responsibility of each operating unit. Although the Computer Security Act and GISRA require that all federal employees having information security-related duties and responsibilities receive job-specific training, the *Commerce Acquisition Manual,* which contains the training requirements for all Commerce contracting personnel, does not include a requirement for security training of any kind.

NIST Special Publication, 800-16, *Information Technology Security Training Requirements,* delineates the training that should be provided for specific information security-related job responsibilities, including acquisition. Using this publication as a guide, information security training should be required for all procurement personnel involved in the acquisition of IT. The Department's procurement executive should enforce information security training requirements, and employee status with regard to this training should be added to the training database maintained by the Office of Acquisition Management. This publication also addresses information security training requirements for another key member of the acquisition team—contracting officers' technical representatives (COTRs).

Conclusion

As outsourcing of IT services increases, the risk of contractors causing security violations—inadvertently or deliberately—also grows. Contracting officers and other acquisition team members need sufficient guidance and training, as well as support from technical experts and program officials, to ensure that they are able to prepare and administer IT service contracts in a way that makes the contractor's responsibility and accountability for safeguarding the government's information assets clear and enforceable.

However, the lack of adequate guidance in the FAR and in its own policies leaves the Department with the significant challenge of developing, implementing, and enforcing policies to ensure that adequate information security requirements are included and followed in all of its IT service contracts. To accomplish this, the Department needs to assess what is required by law and regulation, evaluate guidance generated by other federal agencies,[7] and seek the advice of technical

[7] For example, NASA has recently implemented a requirement for its acquisition plans to include a discussion of information security risks, and for its contracts for IT or IT services to include information security provisions when the contractor will have access to sensitive information in unclassified systems.

experts.[8] The Department must also determine whether current contracts need to be modified to include information security provisions, recognizing that in some cases, contract costs could increase as a result of such changes. Without these actions, the Department will remain without essential tools for protecting the Department's sensitive IT assets and information.

Recommendations

The Chief Financial Officer and Assistant Secretary for Administration should take the necessary actions to ensure that all contracting offices within the Department of Commerce, including USPTO, include adequate information security provisions in all IT service contracts in order to protect the Department's sensitive IT information and assets. To accomplish this, various bureaus, offices, and officials will be required to coordinate their efforts and take the following actions:

1. The Department's procurement executive, with the assistance of the CIO, should develop and disseminate policy for acquisitions of IT systems and services that requires

   a. an assessment of information security risk during the acquisition planning phases;

   b. identification and inclusion of appropriate information security requirements in specifications and work statements;

   c. an assessment, in the proposal evaluations, of the competing contractors' capability to meet those requirements;

   d. inspections to determine the contractor's compliance with information security requirements during contract performance; and

   e. termination of access to systems and networks once the contract is closed out.

   The CFO/ASA has agreed with this recommendation; however, the response noted that the policy would be completed four months from the availability of the update to NIST Special Publication 800-4, *Computer Security Considerations in Federal Procurements*. We believe that the update to the NIST publication should not drive the schedule of the policy, which should be completed as soon as possible. The current version of NIST Special Publication 800-4 is a solid tool that can be used until the updates are completed.

2. The Department's procurement executive, with the assistance of the CIO and in consultation with the Office of General Counsel, should establish standard contract provisions for safeguarding the security of unclassified systems and information and should include such provisions in solicitations and contracts for IT services.

[8]See, for example, *Security for Information Technology Service Contracts*, Carnegie Mellon University. The University's Software Engineering Institute has developed comprehensive guidance for identifying security requirements for IT service contracts and managing these contracts to avoid possible security problems.

The CFO/ASA has agreed with this recommendation. The response noted that some mandatory contract provisions may be subject to the regulatory and information collection process. Given this, the response notes that completion of standard contract provisions is estimated to be June 20, 2003.

3. The Department's procurement executive, with the assistance of program officials and in consultation with the Office of General Counsel, should instruct all heads of contracting offices to review all current contracts and solicitations for IT services to

   a. determine whether they need to be modified or amended to include information security provisions;

   b. modify contracts and amend solicitations, as needed; and

   c. where modifications or amendments are not made, document rationale for not doing so.

   The CFO/ASA has agreed with this recommendation. According to the response, the Department's procurement executive is coordinating an assessment of existing contracts to determine which will require modification to include information security provisions and estimates completing the assessment by August 30, 2002.

4. The Department's procurement executive, in consultation with the CIO and program officials, should ensure that contracting officers, COTRs, and other procurement personnel have appropriate training in information security by

   a. identifying appropriate training requirements for each grade level;

   b. ensuring that this training is provided, as appropriate; and

   c. including the status of security training in the appropriate training database.

   The CFO/ASA has agreed with this recommendation, and indicates that the procurement executive is coordinating with Department's CIO office, which has the lead role in establishing and administering security awareness training. Training is expected to be completed by the end of June 2002. The Department's procurement executive will continue to work with the CIO's office to determine other appropriate training.

5. The Department's procurement executive, with the assistance of the CIO and program officials, should ensure that contracting officers, IT staff, and program officials are made aware of and use NIST Special Publication 800-4, *Computer Security Considerations in Federal Procurements.*

   The CFO/ASA has agreed with this recommendation. The Department's procurement executive plans to expand Procurement Memorandum 2001-02, *Importance of Information Technology Security to Acquisition*, and enlarge its scope to include the NIST Special

Publication 800-4, once that document is updated. We would like to reiterate that even without the updates, the NIST document is a valuable tool and should be used.

cc: Thomas N. Pyke, Jr., Chief Information Officer
Michael S. Sade, Director for Acquisition Management and Procurement Executive
Jerry A. Walz, Chief, Contract Law Division

Attachment

Table 1. Examples of Steps and Guidance for Ensuring Security in IT Service Contracts

CONTRACT PHASE	STEPS AND GUIDANCE[9]
PREAWARD/AWARD 1. Planning/requirements determination 2. Solicitation/development/issuance a. Statement of work b. Evaluation criteria 3. Proposal evaluation 4. Contractor selection	1. Specify security requirements for the technology and services being acquired, including requirements for compliance with agency's security policy. Requirements may include: —Protection against vulnerability to known forms of attack against the technology to be used —Ability to restrict systems administrator-level access to authorized users —Support for a specified type of user authentication (e.g., one-time passwords) —Ability to log activities so that intrusions or attempted intrusions can be detected —Method of remote or onsite access —Contractor liability, including warranting that no Trojan horses or viruses exist 2. Assess potential contractor's capability to meet security requirements. This can be achieved by: —Obtaining references from other customers —Requiring contractor to demonstrate the required capabilities for and approach to security enforcement 3. Ensure that selected contractor's software is installed and configured to operate securely to protect newly installed software and existing systems. Actions may include: —Require secure installation in contract —Require thorough testing before software is installed on agency's operational systems —Prepare to receive contractor software, including Reserving appropriate computing and storage resources, notifying contractor of configuration or operational constraints, and ensuring the ability to revert to the original system configuration —Verify authenticity of the software being installed 5. Require that selected contractor communicate securely with government site when operating remotely. Actions may include: —Authenticating all connections between hosts —Authenticating the contract users —Encrypting all subsequent communications for exchange of sensitive information —Document, monitor, and reset connections 6. Train contractor in agency security practices.

[9] Steps and guidance were derived from *Security for Information Technology Service Contracts*, Software Engineering Institute, Carnegie Mellon University, Report No. CMU/SEI-SIM-003. See this publication or http://www.sei.cmu.edu/pub/documents/sims/pdf/sim003.pdf for more information.

CONTRACT PHASE	STEPS AND GUIDANCE
POSTAWARD/ADMINISTRATION 1. Quality assurance and inspection plan 2. Award fee determination 3. Past performance reporting	1. Control contractor access to systems. Actions may include: —Use separate subnets, filters, or firewalls to restrict traffic —Require explicit scheduling of contractor processing, when possible —Allow contractor connectivity only when scheduled, and disable access at other times 2. Look for unexpected changes to directories and files. Actions may include: —Establish priorities and schedules for examining files —Maintain authoritative reference data for critical files and directories —Verify the integrity of directories and files according to your established schedule —Identify any missing files or directories —Identify new files and directories —Investigate any unexpected changes among those you have identified 3. Inspect systems and network logs. Actions may include: —Establish priorities and schedules for examining logs —Document any unusual entries —Investigate each documented abnormality —Report all confirmed evidences of intrusion (or attempted intrusion) to internal security point of contact —Read security bulletins from trustworthy sources and other security publications regularly 4. Review contractor's performance. Actions may include: —Establish a process for reviewing contractor compliance with specified security requirements —Establish a process for reviewing contractor compliance with your security policy —Conduct periodic reviews to verify contractor compliance —Regularly execute a file system integrity-checking tool —Ensure that no Trojan horses or viruses exist in the contractor software —Review user problem reports
CONTRACT COMPLETION	1. Eliminate contractor's access to systems and networks. Actions may include: —Eliminate contractor physical access to your facilities —Remove contractor authentication and all means of access to your systems —Archive the contractor software configuration —Transfer responsibility, authority, and ownership for the contractor software —Ensure that non-disclosure agreements executed at contract initiation are still in effect —Require that the contractor sign a statement warranting absence of Trojan horses or viruses

Attachment

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

MAY 1 2002

MEMORANDUM FOR: Judith J. Gordon
Assistant Inspector General for Systems Evaluation
Assistant Secretary for Administration

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

SUBJECT: *Information Security Requirements Need to Be Included in the Department's Information Technology Service Contracts* - Draft Inspection Report No. OSE-14788

This memorandum provides our response to the findings and recommendations in your draft report (Attachment A), on information security provisions 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 specifics (i.e. timetables, implementation plans…) to address those concerns and specific recommendations set forth in this, and the final report. Our comments address each of the five recommendations made in the draft report.

RECOMMENDATION #1

We concur with the recommendation that the Chief Financial Officer and Assistant Secretary for Administration should take the necessary actions to ensure that all contracting offices within the Department include adequate information security provisions in all IT service contracts. To accomplish this, the Department's procurement executive (PE) staff in coordination with the Chief Information Office (CIO) staff, will be working to develop and disseminate policy for acquisitions of IT systems and services in order to protect the Department's sensitive IT information and assets. It is projected that completion of this guidance will be four months from the availability of NIST Special Publication 800-4, Computer Security Considerations in Federal Procurements.

RECOMMENDATION #2

We concur with the recommendation. The Department's procurement executive staff, in coordination with the CIO office and in consultation with the Office of General Counsel (OGC), will work to establish standard contract provisions for safeguarding the security of unclassified systems and information for inclusion in solicitations and contracts for IT services. Note that some mandatory standard contract provisions may be subject to the regulatory and information collection process. Based on anticipated clearance requirements the completion of standard contract provisions is estimated to be June 30, 2003.

RECOMMENDATION #3

We agree with the recommendation and the Department's procurement executive staff is coordinating an assessment of the Department's existing contracts for IT services to determine which contracts will require modification to include information security provisions. The assessment is anticipated for completion by August 30, 2002.

RECOMMENDATION #4

It is critical that contracting officers, COTRs, and other procurement personnel in the Department have appropriate training in information security. The Department's procurement executive staff is already coordinating with the CIO office, which has the lead role in establishing and administering a security awareness-training program for the Department's personnel. This training program is slated for completion by the end of June 2002. Additionally, the Department's procurement executive staff will continue to work with the CIO office to determine what other training might be appropriate.

RECOMMENDATION #5

We concur with the recommendation. The Department's procurement executive staff in coordination with the CIO office, and program officials, will be working to ensure that contracting officers, IT staff, and program officials are made aware of and use NIST Special Publication 800-4, Computer Security Considerations in Federal Procurements. Specifically, the Department's procurement executive staff will expand the existing procurement memorandum (PM) to the Heads of Contracting Offices which stresses the importance of information technology security to acquisition, and enlarge the scope of the PM to include the NIST Special Publication 800-4 document once NIST completes the update.

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 call Mike Sade at (202) 482-4248.

Attachment