U.S. DEPARTMENT OF COMMERCE
Office of Inspector General

U.S. PATENT AND TRADEMARK OFFICE

Information Security in Contracts Needs Better Enforcement and Oversight

Final Inspection Report No. OSE-17455
September 2005

PUBLIC RELEASE

Office of Systems Evaluation

CONTENTS

EXECUTIVE SUMMARY

The Federal Information Security Management Act (FISMA) requires agencies to develop and implement programs to protect information and information technology (IT) systems. FISMA requirements apply to all federal contractors who use federal information, or operate or have access to federal information systems on behalf of an agency. The Office of Management and Budget (OMB) has cited contractor security as a government-wide challenge since 2001and has directed agencies and the OIG to report on agency oversight of contractor IT security.

In response to findings and recommendations made by OIG in May 2002,[1] the Department issued two contract clauses containing IT security requirements. USPTO, as part of its information security program, adopted these clauses to protect information and IT systems from risks posed by contractors who connect to its network or process or store sensitive agency information. The clauses require contractors to comply with USPTO's IT security handbook, have their IT systems certified and accredited,[2] and have their employees undergo appropriate background screening.

We conducted our evaluation to determine whether USPTO had incorporated the two security clauses into IT service contracts and to evaluate the implementation of the clause requirements. We found that most contracts in our sample contained the clauses and that contractor employees receive IT security awareness training. However, USPTO is not properly implementing key requirements in the clauses and in some cases is not enforcing them. Specifically, USPTO designated all contracts in our sample as low risk, even though the relevant criteria suggest that some contracts should have high or moderate risk designations. In these cases, contractors did not receive the appropriate background screening. In addition, contractors have not submitted certification and accreditation packages, and therefore no contractor IT system has been certified or accredited.

We recommend that the Under Secretary of Commerce for Intellectual Property and Director of the U.S. Patent and Trademark Office direct appropriate management officials to ensure that contractor IT security is improved by, among other things, developing plans for establishing appropriate risk designations for contracts and certifying and accrediting contractor systems. (See page 12.)

…

In its September 29, 2005, response to our draft report, USPTO generally concurred with our findings and outlined the corrective actions planned or underway for each recommendation. We synopsize USPTO's response following each recommendation (see pp. 11-12), and in one

[1] 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.* Report No. OSE-14788.

[2] Certification is the comprehensive assessment of the management, operational, and technical controls of an information system to determine if the controls are implemented correctly, operating as intended, and producing the desired outcome. Accreditation is management's formal authorization to allow a system to operate, and acceptance of remaining system vulnerabilities.

instance, we provide a comment on the response. USPTO's complete response is included as an attachment to this report. The actions identified by USPTO are responsive to our recommendations and when implemented should improve IT security for contractor employees and contractor systems.

INTRODUCTION

The Federal Information Security Management Act (FISMA)[3] requires agencies to develop and implement programs to protect information and information technology (IT) systems. As agencies increasingly rely on contractors to support their missions, it has become apparent that risks to government information and IT systems could be introduced through contractor employees and their IT systems. For example, contractor operations may lead to

- Unauthorized modifications to information;
- Introduction of malicious software;
- Unauthorized disclosure of, or access to, sensitive information; and
- Disruption to government operations by IT system failures or denial of access.[4]

FISMA requires agencies to review their information security program annually and Offices of Inspector General (OIGs) to independently evaluate agency IT security programs. How these programs are being applied to contractors is a focus of this year's FISMA reporting instructions issued by the Office of Management and Budget (OMB): Chief Information Officers (CIOs) and OIGs are directed to report on agency oversight of contractor IT security. OMB's instructions emphasize that contractors' IT security procedures must be "identical, not equivalent" to those of federal agencies. In support of our 2005 FISMA reporting requirements, we evaluated USPTO's efforts to implement IT security requirements for contractor employees and systems.

USPTO plays an integral role in the nation's intellectual property system. As part of its mission, the agency is responsible for awarding and protecting patents and trademarks. To perform these functions better, USPTO's *21st Century Strategic Plan* calls for total electronic processing for patents and trademarks. Because the information contained in both is critical to protecting the rights of patent/trademark holders and can impact significant business investment decisions, USPTO systems need to safeguard the confidentiality, integrity, and availability of the information. USPTO relies heavily on contractor employees and IT systems to accomplish this transformation and support operations.

USPTO IT Security Policy

USPTO's IT security policy, Agency Administrative Order No. 212-4, aims to establish a secure IT environment to protect agency information and IT systems. The policy applies to both USPTO employees and contractors, and authorized creation of the IT security handbook. The handbook identifies specific security practices and refers to specific procedures contained in the agency's technical standards and guidelines.

[3] *Title III, E-Government Act of 2002* (P.L. 107-347).

[4] U.S. Government Accountability Office, April 2005. *Information Security: Improving Oversight of Access to Federal Systems and Data by Contractors Can Reduce Risk.*

IT Security Clauses

In response to a May 2002 OIG report,[5] which found that Commerce contracts frequently lacked adequate security provisions, the Department issued two contract clauses containing IT security requirements:

- ***Security Requirements for Information Technology Resources*** **(Commerce Acquisition Regulations** (CAR) 1352.239-73) (clause 73).

- ***Security Processing Requirements for Contractors/Subcontractor Personnel for Accessing DOC Information Technology*** (CAR 1352.239-74) (clause 74).

USPTO modified these clauses to reference its own policy and guidance without changing their substantive requirements. Clause 73 requires that contractors comply with USPTO's IT security handbook; submit a certification and accreditation (C&A)[6] package 14 days after contract award for systems that connect with USPTO networks, or process or store sensitive information; and that USPTO approve or reject the C&A package. Clause 74 requires security awareness training for contractor personnel and designation of the contract risk level (i.e., high, moderate, or low) to define the type of background screening needed. In late 2003, the USPTO Office of Procurement directed contracting officers to incorporate clauses 73 and 74 into all new service contracts, as well as to insert clause 74 into all existing service contracts and clause 73 into all applicable existing contracts.[7]

Roles and Responsibilities

The task of imposing security requirements on contractors relies on the expertise of USPTO personnel spread across several operating units, as follows:

Office of Procurement/Contracting Officers

- Authorized to enter into and modify contracts.
- Responsible for contractor compliance with contract terms and for safeguarding USPTO interests in procurements.
- Appoint contracting officer's representative (COR).

---

[5] 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.* Report No. OSE-14788. A subsequent OIG evaluation found that the Department had made progress in incorporating the new IT security clauses into contracts, but provisions for controlling contractor access to Department systems and networks were generally absent, and there was little evidence of contract oversight or of coordination among contracting, technical, and information security personnel. (U.S. Department of Commerce Office of Inspector General, September 2004. *Office of The Secretary: Information Security in Information Technology Security Contracts Is Improving, but Additional Efforts Are Needed.* Report No. OSE-16513).

[6] Certification is the comprehensive assessment of the management, operational, and technical controls of an information system to determine if the controls are implemented correctly, operating as intended, and producing the desired outcome. Accreditation is management's formal authorization to allow a system to operate, and acceptance of remaining system vulnerabilities.

[7] USPTO Office of Procurement told us that it modified about 35 contracts in early 2004 to include both clauses.

Office of Chief Information Officer - Office of Acquisition Management (OCIO-OAM)

- Directs the acquisition of IT products and services to support, develop, and maintain USPTO automated information systems.
- Serves as COR for USPTO-wide IT contracts, providing day-to-day contract administration.

OCIO - IT Security Program Office (ITSPO)

- Develops and implements IT security to safeguard USPTO information and IT systems.
- Provides IT security guidance and technical assistance.
- Works with contractors to establish access to USPTO network and IT systems.

Office of Security

- Provides leadership on USPTO security programs.
- Processes personnel security/suitability and security clearances.
- Completes contractor suitability investigations.

Operating Unit Personnel

- Determine potential adverse impact on an organization if there is a breach of security.
- Define contract requirements, which in turn determine contract risk designation and whether certification and accreditation of contractor IT system is required.
- Senior manager serves as authorizing official for the accreditation of contractor IT systems.

OBJECTIVES, SCOPE, AND METHODOLOGY

The objective of this review was to determine whether clauses 73 and 74 have been incorporated into IT service contracts and how USPTO has implemented their requirements, particularly in contracts that may require contractor systems to connect with the USPTO network or that allow contractor systems to access or store sensitive information.

To satisfy our objective, we selected a judgmental sample of 10 current contracts from listings provided by USPTO and the Department. The estimated value of the sample is $1.7 billion. (See table 1.) We reviewed contract files to determine whether the contracts contained the clauses and interviewed managers and staff from the Office of Procurement, OCIO-OAM, OCIO-ITSPO, Patent Office, and Office of Security.

Table 1. Contract Sample

Contract Description	Number of Contractors	Estimated Value (in $ millions)
IT product assurance	1	3
Systems Engineering and Technical Assistance (SETA)	2	72
Systems Development and Integration (SDI)	2	530
Patent Data Capture	1	876
System engineering for proprietary software	1	5
Agency-wide administrative support services	1	192
Policy development for electronic filing and records management	1	5
Network vulnerability testing	1	Less than 100K
Total Estimated Value		**$1.7 billion**

Source: Estimated values obtained from list of IT service contracts provided by USPTO Office of Procurement, April 7, 2005.

As our evaluation criteria, we used clauses 73 and 74, FISMA, Commerce's IT Security Program Policy and Minimum Implementation Standards, USPTO's IT security policy, and NIST guidance. We conducted our evaluation in accordance with the Inspector General Act of 1978, as amended, and the Quality Standards for Inspections issued by the President's Council on Integrity and Efficiency. We performed our fieldwork between April 2005 and July 2005.

FINDINGS AND RECOMMENDATIONS

I. Most USPTO Contracts Include IT Security Clauses, but Important Requirements Are Not Implemented Properly or Are Not Enforced

We found that most of the contracts we reviewed contain the IT security clauses and that contractor employees receive IT security awareness training. However, USPTO is not properly implementing key requirements in the clauses and in some cases is not enforcing them. For example, the agency designated all contracts in our sample as low risk—meaning contract employees undergo a minimal background investigation, but the relevant *Commerce Acquisition Manual* (CAM) criteria suggest that some contracts should have high or moderate risk level designations; thus, many contractor employees should receive more rigorous background screenings commensurate with the potential impact an individual in that position could have on USPTO operations. Moreover, contractors have not submitted C&A packages, and therefore none of their systems has undergone certification testing or received accreditation.

A. USPTO Has Incorporated the IT Security Clauses into Most Contracts

Eight of the 10 contracts in our sample contained both IT security clauses. Among the 8 were recently awarded contracts as well as several that were in effect in 2004 but had been modified to include the clauses. USPTO did not document its decisions to keep the clauses out of the remaining 2 contracts, so we asked agency personnel to explain the rationale for the exclusions. They stated that in one case, the contractor was not connected to the USPTO network and did not have access to sensitive agency information. Therefore, the requirements of the clauses were not applicable. There are currently no open task orders under this contract, but if new task orders are issued, USPTO needs to evaluate whether the contractor will have access to sensitive information or connectivity to its network and should add the clauses as warranted.

The other contract was a task order under a General Services Administration (GSA) contract for IT security vulnerability testing.[8] The project manager stated that the clauses were not included because the nature of the contract work would cause the contractor to violate the IT security requirements established by clause 73.

We do not agree with the decision to exclude the clauses from this task order because the work it authorized gave the contractor access to USPTO systems and generated sensitive data. Yet, the contractor's personnel were not subject to background screening, and the contractor's systems were not certified and accredited. USPTO subsequently released another solicitation for vulnerability testing that did not contain the IT security clauses under a GSA contract, but agreed after our discussions with the contracting officer, to incorporate clauses 73 and 74 into the solicitation. We remain concerned, however, that there may be other task orders under government-wide contracts that should, but do not, contain the IT security clauses and that USPTO's contract review and oversight processes are not ensuring that they are added.

[8] The task order states that the contractor would mimic an external attacker trying to penetrate the target systems, which contain sensitive but unclassified USPTO data.

B. Contract Risk Levels Are Not Designated Correctly, and Background Screenings May Be Too Low for Many Contractor Employees

One way the government has traditionally sought to protect its assets is to subject employees to background screening. The level of scrutiny a federal employee receives is dictated by the sensitivity of the position he holds—that is, the damage an individual, by virtue of his position, could cause to the efficiency or integrity of agency operations or national security. As the government's reliance on contractors has increased, contractor employees working at government facilities have been subjected to screening as well. Clause 74 expands this requirement by mandating screening, regardless of location, for contractor employees who have access to government IT systems or who use IT systems that are interconnected with agency networks.

Contractor screening is based on the level of risk to the government posed by the contract. The associated risk designation (high, moderate, or low) defines the extent of screening. Clause 74 provides that contract risk level determinations be made in accordance with section 1337.70 of the *Commerce Acquisition Manual* (CAM).[9] The appendix to this report presents the current CAM criteria for designating contract risk levels. It should be noted, however, that these criteria are undergoing change in response to a new security control framework developed by NIST.[10] With the new framework, risk is to be determined not only by the function an individual performs, but also by the potential impact on an organization should certain events occur that jeopardize information and information systems. The Department's CIO has adopted the new framework in the recently-revised Commerce IT security policy and has initiated an effort to have the relevant Departmental suitability, security, and acquisition policies and guidance updated accordingly.

USPTO designated all the contracts in our sample as low risk. As a result, the employees working under these contracts were subject to a National Agency Check and Inquiries (NACI) investigation, one of the least comprehensive screening levels. As shown in table 2, the relevant CAM criteria suggest that some contracts in our sample should have high or moderate risk level designations. For example, the patent data capture contract gives contractors access to patent applications before they are published. Because the potential to unfairly exploit the information contained in patent applications is so great, federal law, 35 USC 122, prohibits its disclosure.

We were unable to determine USPTO's criteria for designating contract risk levels because the contract files contained no documentation regarding the determinations. To understand these decisions, we discussed the designations with agency personnel, who offered two explanations:

- USPTO information is not classified or designated national critical, so higher risk designations are unnecessary.

[9] CAM 1337.70 directs a program office representative, typically the COR, to make contract risk level designations in conjunction with operating unit management, office of security, and the procurement office. In section (a)5 of clause 74 states that the contracting officer makes contract risk level designations.

[10] NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*, February 2005.

- Agency personnel who manage the contracts or perform similar work are in positions designated low risk; therefore, contractor employees should have the same risk designations as their agency counterparts.

While these explanations may have contributed to improper risk level determinations, an agency-wide preference for operating in a low-risk environment appears to underlie the problem. The low-risk designations of the contracts in the sample are not anomalies. USPTO senior managers told us that nearly all agency contracts are designated low risk. Further, an overwhelming percentage of USPTO positions are similarly designated low risk. USPTO's IT security handbook strongly favors low-risk designations, stating that agency contracts should require NACI screening. The handbook neither provides high or moderate risk designations as alternatives, nor does it describe when high or moderate risk designations are appropriate.

Table 2. USPTO Risk-Level Designation Compared to CAM Criteria

Contract Work Description	USPTO Risk Level	CAM Risk Level	Relevant CAM Criteria
System Design and Integration (SDI) contracts–System design and development, allowing access to operational systems and underlying IT infrastructure. (2 contracts)	Low	High	Designing and operating a computer system that includes ADP hardware, software, and/or data communications, regardless of the sensitivity of the data. Access to a computer system that could result in grave damage or in personal gain.
Patent Data Capture contract–Managing patent applications, allowing access to pre-publication patent applications, confidentiality required by 35 USC 122. (1 contract)	Low	High Moderate	Access to a computer system during the operation or maintenance process that could result in grave damage or in personal gain. Work involving access to sensitive information.
System Engineering and Technical Assistance contract (SETA)–Developing and implementing USPTO IT security program, allowing access to security plans, and proprietary/confidential information. (1 contract)	Low	High	Planning and implementing a computer security program

At our exit conference, USPTO officials expressed serious concerns about the possibility of having more comprehensive background screenings than the NACI investigation, as described above, citing the financial burden as well as delays in performing work while screenings are being performed, which they believe could impact operations. We note, however, that after pre-employment checks, clause 74 and CAM 1337.70 both allow contractors and employees to start work prior to completion of the appropriate investigation so long as the process is initiated 3 days after work commences. This is not to diminish the importance of investigative screening, but rather gives agencies some flexibility to secure agency assets and information while maintaining operations.[11] Another flexibility is that even if a contract is designed as high or medium risk, some employees may be screened at a lower level as appropriate for their work as

[11] Clause 74 states, "At the option of the government, interim access to DOC IT systems may be granted pending favorable completion of a pre-employment check. Final access may be granted only on completion of an appropriate investigation based upon the risk level assigned to the contract by the Contracting Officer."

long as adequate controls are established to ensure they do not perform higher risk work, or gain access to information or systems for which they are not screened. USPTO needs to develop a plan and schedule for reviewing contract risk designations and modifying them as appropriate.

Completing appropriate background screening is the initial step in overseeing contract IT security. Background screening is designed to identify individuals who pose a risk to government assets and operations based on past conduct and associations. However, screening alone does not effectively safeguard government information and IT systems because individuals who have successfully passed the screening process can introduce risks, either intentionally or not. Vulnerabilities in contractor systems that contain sensitive agency information or connect to an agency network can disrupt agency operations or allow unauthorized access to information. Certifying and accrediting contractor systems guards against such threats by ensuring technical, operational, and management controls work as intended.

C. Failure to Certify and Accredit Contractor Systems Places USPTO at Risk

Certification and accreditation is an integral part of an agency's information security program. Certification is the formal testing of an IT system's security controls to determine whether they are operating as intended and producing the desired outcome. With this information, agencies can decide, based on risk, how best to minimize the potential for disruption to operations. Accreditation is management's formal authorization to allow a system to operate, and acceptance of remaining system vulnerabilities.

Contractor Systems Are Not Certified or Accredited

Departmental and USPTO IT security programs provide for IT system certification and accreditation. Clause 73 requires contractor IT systems to undergo the C&A process when they either are connected to a USPTO network, or process or store sensitive agency data. The C&A package must be submitted within 14 days after contract award.[12] Packages must include a risk assessment, system security plan, contingency plan, system test plan and test results, and the certifier's recommendation.

None of the USPTO contractor systems including those in our sample has been certified and accredited, nor had any of the contractors submitted a C&A package,[13] even though the 14-day deadline for submission has long passed. The failure to certify and accredit contractor systems is particularly troubling because most systems in our sample are operational and connected to the USPTO network or contain sensitive agency data without the assurance that they are adequately secure.

[12] After we completed our fieldwork for this report, we met with officials from the Department's OCIO and OAM to raise concerns about the feasibility of the 14-day deadline. They told us that the Department is considering ways to improve implementation of the C&A requirement and are aware that 14 days to complete a certification and accreditation package is unreasonable. The Department's IT Security Program Manager is interpreting the 14 days to be for the contractor to submit to the agency its detailed plans for completing the certification and accreditation process.

[13] One contractor submitted elements of a draft C&A package in September 2004, but no further action was taken on it after the ITSPO proposed revisions.

We are not the first to raise concerns about the risks of USPTO contractor systems and compliance with IT security requirements. Last September, the agency issued a report of its own, summarizing vulnerabilities of contractor systems in all security control areas. The report's primary recommendation was for USPTO to better enforce existing IT security contract requirements.[14]

Factors Contributing to Noncompliance with the C&A Requirement

Several factors explain why contractors have ignored the C&A requirement:

- USPTO did not clearly communicate the magnitude and importance of the C&A requirement in contract solicitations and modifications.

- Once clause 73 was in the contracts, the agency did not administer the C&A requirement in a manner that promoted compliance.

- None of the involved USPTO operating units provided the leadership necessary to coordinate the roles of contracting officers, CORs, and ITSPO. This coordination is required since various individuals have complementary roles in overseeing contractors' adherence to security policies.

Each point is discussed in more detail below.

Failure to communicate the magnitude and importance of the C&A requirement. Clause 73 establishes a 14-day deadline for submission of the C&A package because of the potential for disruption to government operations once work under the contract begins. Contractors must recognize and understand C&A requirements when solicitations are issued or contracts are modified. Below, we identify several ways contractors' awareness of the C&A requirement could have been improved:

- **Contract Deliverable.** The C&A package was not identified as a deliverable in solicitations or contract modifications. Had it been, contractors might have recognized that submission of the C&A package was part of the required contract performance.

- **Application of the Requirement.** When USPTO modified contracts to include the C&A requirement, it did not formally advise contractors whether the requirement applied. About 35 contracts were modified in March 2004 to include clause 73, but the C&A requirement did not apply to all 35. Some contractors may have been unsure about whether the requirement applied to them.

- **Elements of a C&A Package.** Clause 73 references additional guidance on the elements of a C&A package, but such reference, by itself, is insufficient to clearly communicate the complexity of the C&A effort, which is a new undertaking for many contractors.

[14] USPTO, September 17, 2004. *USPTO Contractor Facilities Security Assessment Executive Overview.*

Specific direction on what a C&A package must contain should have accompanied solicitations and contract modifications. USPTO needs to provide C&A guidance that meets OMB's directive that contractors and federal agencies have "identical, not equivalent" IT security procedures.

- **C&A Costs.** USPTO did not develop cost estimates for certifying and accrediting contractor systems. Without estimates, a fixed price for contractors' C&A efforts could not be established. Contractors whose contracts were modified by the addition of clause 73 would have been more attentive to the C&A requirements if a fixed price was associated with the effort. Various USPTO personnel told us that cost has not been an issue for contractors; perhaps this is because contractors have done little to comply with the C&A requirement. Some USPTO personnel acknowledged knowing first-hand of the significant cost and time necessary to complete C&A. Without estimates or established contract prices, there is greater uncertainty as to USPTO's financial liability for implementation of the C&A requirement. In the event that contractors seek additional funding to comply with the C&A requirement, USPTO could pay more than it otherwise would have because there is no contract pricing or cost estimates for assessing the reasonableness of contractors C&A costs.

Failure to administer the C&A requirement in a manner that promoted contractor compliance. Even though the C&A requirement was added to contracts, contractors were not given reason to think certification and accreditation was a USPTO priority. For all the contracts in the sample, the 14-day deadline passed without submission of C&A packages.[15] From our review of contract files and requests for USPTO documents, we found no documentation indicating that, prior to expiration of the deadline, USPTO:

- Warned contractors the deadline was approaching;
- Informed them that clause 73 allows for contract termination when they do not satisfy the C&A requirement; or
- Extended the deadline, or informed contractors that a new deadline would be established.

After the deadlines expired, no money was withheld for not submitting C&A packages, nor was access to sensitive information or the USPTO network curtailed. By not using any of the tools available to address noncompliance with the contracts, contractors came to the conclusion that the C&A process was not a priority for USPTO.

Failure to coordinate the roles of contracting officers, CORs, and ITSPO. Finally, the absence of strong leadership from USPTO personnel responsible for implementing contractor IT security contributed to the noncompliance with C&A requirement. At the time of our fieldwork, ITSPO personnel were working to secure contractor connectivity to the agency's network and provide detailed direction on C&A packages. The difficulty of this effort, which was directed toward a single contractor, highlights the need for coordination among the USPTO operating units overseeing contractor IT security. ITSPO provided us with a copy of a draft appendix to the IT security handbook, which attempts to delineate responsibilities for IT security in contracts. As

[15] See footnote 10.

noted in our September 2004 report on contractor IT security,[16] contracting officers, CORs, system owners, and ITSPO have significant and complementary roles in overseeing contractors' adherence to appropriate security policies. These individuals need to work together to protect USPTO operations from potential risks arising from contractors' network connectivity or access to sensitive information. While USPTO ultimately must decide the best way to coordinate oversight of contractor IT security, the CORs' familiarity with the operational needs of the agency, the contractor, and various security issues appear to make the COR position a strong candidate for taking the lead in coordinating the involvement of the various individuals involved in contractor IT security oversight.

Recommendations

The Under Secretary of Commerce for Intellectual Property and Director of the U.S. Patent and Trademark Office should direct appropriate management officials to ensure that:

1. A plan and schedule are developed for certifying and accrediting contractor systems that connect to the USPTO network, or process or access sensitive agency information.

    a. As part of the planning, develop cost estimates for addressing USPTO budget needs and contractor funding requests.
    b. Improve communication with contractors so they are fully aware of specific C&A requirements and USPTO expectations.

Synopsis of USPTO's Response.
USPTO agreed with this recommendation. USPTO stated that it would work with the Department CIO Office and OIG to establish criteria for determining risk levels. USPTO also indicated that it would develop a plan and schedule for identifying contractor systems requiring C&A and for performing C&A. USPTO intends to develop procedures to improve communications with contractors about C&A requirements and to identify the C&A requirements as a priced deliverable in solicitations or contract modifications.

2. Contractor systems are certified and accredited in accordance with FISMA and implementing regulations.

    a. Designate appropriate USPTO program officials responsible for accrediting systems.
    b. Assign USPTO personnel to participate in the certification process.
    c. Test security control at a level that corresponds to risks associated with the system.

Synopsis of USPTO's Response.
USPTO agreed with this recommendation, stating that it will review risk designations, designate a program official to oversee contractor C&A activities, and assign USPTO personnel to participate in all aspects of contractor C&A efforts. USPTO also pointed out that NIST Special

[16] U.S. Department of Commerce Office of Inspector General, September 2004. *Office of the Secretary: Information Security in Information Technology Security Contracts Is Improving, but Additional Efforts Are Needed*, OSE-16513.

Publication 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, generally sets sensitivity data for intellectual property at the "low" level.

OIG Comment on USPTO Response.
It should be recognized that while NIST Special Publication 800-60 generally sets sensitivity levels for intellectual property as "low," this guidance specifically identifies pre-published patent applications as having a moderate impact level and identifies 35 U.S.C. § 122 as a Federal statute requiring protection of pre-publication from disclosure.[17]

3. CORs, managers, and security officers understand the criteria for determining appropriate contract risk level designations.

Synopsis of USPTO's Response.
USPTO agreed with this recommendation. USPTO stated that it would develop guidelines, to include documentation of decision making, to implement criteria for determining contract risk level designations.

4. A plan and schedule are developed for reviewing existing contract risk designations and modifying them as appropriate.

Synopsis of USPTO's Response.
USPTO agreed with this recommendation. USPTO stated that it would review existing contract risk level designations and make modifications where appropriate.

5. IT security clauses are incorporated into all new task orders under government-wide service contracts.

Synopsis of USPTO's Response.
USPTO agreed with this recommendation. USPTO stated that it will review task orders under government-wide contracts for compliance with contractor IT security requirements and include a line item for C&A deliverables where appropriate.

6. The draft appendix in the IT security handbook—which establishes roles and responsibilities for implementing IT security in acquisitions—is reviewed and modified as needed.

Synopsis of USPTO's Response.
USPTO agreed with this recommendation. USPTO stated that OCIO has revised Appendix W for review within USPTO and that final updates will be made as needed.

[17] NIST Special Publication 800-60, *Volume II: Appendixes to Guide for Mapping Types of Information and Information Systems to Security Categories*, June 2004, pp. 215-216 and Appendix E.

Appendix

Risk Levels for Nonclassified Contracts

Criteria from Commerce Acquisition Manual 1337.70, Attachment 1
"Security Processing Requirements for On-Site Service Contracts"

High Risk

- Work which involves continuous foreign travel of 90 days or more under the auspices of DOC;
- Work involved in functions or in operations of the Department that are critical to the accomplishment of the mission of the Department;
- Work involved in investigative, compliance, or senior level auditing duties;
- Work which occurs during restricted hours within a DOC building which houses classified information or equipment, and which is not supervised by an appropriately cleared government employee, where appropriate physical security measures are not in place to prevent unauthorized disclosure;
- Work which involves fiduciary, public contact, or other duties involving the highest degree of public trust;
- ADP work involved in:
    - Planning, directing, and implementing a computer security program;
    - Directing, planning, designing, and operating a computer system that includes ADP hardware, software, and/or data communications, regardless of the sensitivity or classification of the information stored on the system; or
    - Access to a computer system, during the operation or maintenance process, that could result in grave damage or in personal gain; and
    - Any other work designated High Risk by the contracting officer or the head of the operating unit or departmental office.

Moderate Risk

- Work which involves free access and movement within a DOC building which houses classified information or equipment during normal work hours with little or no supervision by an appropriately cleared government employee;
- Work which occurs during restricted hours within a DOC building which houses classified or sensitive information or equipment even though supervised by a government employee;
- ADP work in which the incumbent will be responsible for the direction, planning, design, operation, or maintenance of a computer system, and whose work is technically reviewed by government personnel processed at the Critical–Sensitive level or above to ensure the integrity of the system;
- Work which requires access to sensitive information (information protected under the Privacy Act or Title 13, etc); and
- Work involving foreign travel less than 90 days duration.

Low Risk

Work that does not fall into any of the above categories and would be equivalent to a low risk designation if the individual was performing the work as an employee.

Attachment

UNITED STATES PATENT AND TRADEMARK OFFICE

UNDER SECRETARY OF COMMERCE FOR INTELLECTUAL PROPERTY AND
DIRECTOR OF THE UNITED STATES PATENT AND TRADEMARK OFFICE

SEP 29 2005

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

FROM: Jon W. Dudas Stephen Pinkos for Jon Dudas
Under Secretary of Commerce for Intellectual Property and
Director of the United States Patent and Trademark Office

SUBJECT: Response to Draft Report No. OSE-17455: "*United States Patent and Trademark Office: Information Security in Contracts Needs Better Enforcement and Oversight*"

This memorandum provides our response to the findings and recommendations in your draft report on information security in United States Patent and Trademark Office (USPTO) contracts.

In general, the USPTO agrees with the findings and conclusions found in the subject draft report. For each of the recommendations made in the draft report, we include a summary of the proposed corrective actions we plan to take to address and implement each recommendation.

Recommendation #1: A plan and schedule are developed for certifying and accrediting contractor systems that connect to the USPTO network, or process or access sensitive agency information.

a) As part of the planning, develop cost estimates for addressing USPTO budget needs and contractor funding requests.
b) Improve communication with contractors so they are fully aware of specific Certification and Accreditation (C&A) requirements and USPTO expectations.

USPTO Response: We agree. The USPTO will work with the Department of Commerce (DOC) Office of the Chief Information Officer (OCIO) and Office of Inspector General (OIG) to establish clear guidelines or criteria for what constitutes the various risk levels. Key actions include:

- Developing a plan and schedule for certifying and accrediting contractor systems that are connected to the USPTO network;

- Developing a plan for how to review the existing inventory of contractor Information Technology (IT) systems, validate the appropriate risk level, and establish system costs and a schedule to conduct the C&A activity;
- Developing procedures to communicate to prospective contractors the contents, magnitude and importance of the C&A requirement which will be developed and put in place;
- Identifying the C&A requirements as a priced deliverable in solicitations or contract modifications.

Recommendation #2: Contractor systems are certified and accredited in accordance with Federal Information Security Management Act (FISMA) and implementing regulations.

a) Designate appropriate USPTO program officials responsible for accrediting systems.
b) Assign USPTO personnel to participate in the certification process.
c) Test security control at a level that corresponds to risks associated with the system.

USPTO Response: We agree to review all risk designations; however, we note that National Institute of Standards and Technology (NIST) Instruction 800-60 (attached), generally sets sensitivity data for intellectual property at the "low" level. Nonetheless, we will work with the DOC to establish guidelines and apply all relevant FISMA implementation guidance to existing USPTO contracts to determine the appropriate risk level. Key actions include:

- Reviewing the existing USPTO systems and data (in concert with guidelines developed with DOC above) to determine the appropriate security levels;
- Designating a USPTO program official who will be responsible for ensuring that the guidance developed is followed for all contracts that are identified as requiring C&A activity;
- Assigning USPTO personnel to participate in all aspects of the certification process with the contractor, to include testing of the system controls.

Recommendation #3: Contracting Officer Technical Representatives (COTRs), managers, and security officers understand the criteria for determining appropriate contract risk level designations.

USPTO Response: We agree. Key actions include:

- Preparing and disseminating information based on the guidelines established above, to COTRs, task managers, and security officers regarding the criteria for determining appropriate contract risk level designations;
- Establishing clear guidance on documenting and filing the determination regarding contract risk levels.

Recommendation #4: A plan and schedule are developed for reviewing existing contract risk designations and modifying them as appropriate.

USPTO Response: We agree. Key actions include:

- Developing an action plan and schedule for completing the contract reviews and modifications;
- Identifying those contracts covered by the risk designations;
- Reviewing all relevant contracts to determine if the proper risk level designation has been applied;
- Modifying those contracts designated at inappropriate levels.

Recommendation #5: IT security clauses are incorporated into all new task orders under government-wide service contracts.

USPTO Response: We agree. Key actions include:

- Reviewing each request for contractual action to determine that the proper risk level designation has been assigned and documented;
- Adding the appropriate clauses with risk level designations in the solicitation;
- Including a line item, or items, in the pricing schedule for the deliverables required by the clauses.

Recommendation #6: The draft appendix in the IT security handbook – which establishes roles and responsibilities for implementing IT security in acquisitions – is reviewed and modified as needed.

USPTO Response: We agree with the recommendation. The USPTO OCIO has drafted a revised Appendix W for review within USPTO. The Appendix W will be updated to include a description of the appropriate use of high or moderate risk designations as alternatives, when these are appropriate.

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 Barry Hudson, Deputy Chief Financial Officer on 571-272-9200.

Attachment

NIST Special Publication 800-60
Version 2.0

NIST

National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

Volume II: Appendixes to Guide for Mapping Types of Information and Information Systems to Security Categories

William C. Barker
Annabelle Lee

INFORMATION SECURITY

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

June 2004

U.S. DEPARTMENT OF COMMERCE
Donald L. Evans, Secretary

TECHNOLOGY ADMINISTRATION
Phillip J. Bond, Under Secretary of Commerce for Technology

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
Arden L. Bement, Jr., Director

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. The consequences of unauthorized modification or destruction of business and industry development information may depend on the urgency with which the information is typically needed.

Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect operations and/or public confidence in the agency, but the damage to the mission would usually be limited.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for most business and industry development information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to business and industry development information. Missions supported by business and industry development information are generally tolerant of delay.

Recommended Availability Impact Level: The provisional availability impact level recommended for business and industry development information is ***low***.

D.9.2 Intellectual Property Protection Information Type

Intellectual property protection involves law enforcement activities involving the enforcement of intellectual property including inventions, literary and artistic works, and symbols, names, images, and designs used in commerce. Note that intellectual property protection is an exception to the often-close relationship between impacts to law enforcement information and information systems and the security of critical infrastructures and key national assets. The following security categorization is recommended for the intellectual property protection information type:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of intellectual property protection information on the abilities of responsible agencies to enforce intellectual property including inventions, literary and artistic works, and symbols, names, images, and designs used in commerce. The consequences of unauthorized disclosure of the majority of intellectual property protection information will result in, at most, a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: There are legislative mandates prohibiting unauthorized disclosure of trade secrets. Trade secrets will generally be assigned a ***moderate*** confidentiality impact level. In the case of patent activities, technical details of applications involving inventions with military applications and with deliberations concerning withholding patents as a result of *national security* considerations may be sensitive. (In some

cases, the patent application information may be classified or to contain information concerning weapons or weapons systems. In such cases, the information would be *national security information,* and outside the scope of this guideline.)

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for intellectual property protection information is ***low***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. The consequences of unauthorized modification or destruction of intellectual property protection information depends on the criticality of the information with respect to agency mission capability, protection of agency assets, and safety of individuals. The effects of modification or deletion of this information are generally limited with respect to agency mission capabilities or assets.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for intellectual property protection information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to intellectual property protection information. The nature of intellectual property protection processes is tolerant of reasonable delays.

Recommended Availability Impact Level: The provisional availability impact level recommended for intellectual property protection information is ***low***.

D.9.3 Financial Sector Oversight Information Type

Financial Sector Oversight involves the regulation of private sector firms and markets (stock exchanges, corporations, etc.) to protect investors from fraud, monopolies, and illegal behavior. This also includes deposit protection. The recommended provisional categorization of the financial sector oversight information type follows:

Security Category = {(confidentiality, Moderate), (integrity, Low), (availability, Low)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of financial sector oversight information on the ability of responsible agencies to regulate private sector firms and markets (stock exchanges, corporations, etc.) to protect investors from fraud, monopolies, and illegal behavior. This also includes deposit protection, creation, regulation, and control of the nation's currency and coinage supply and demand.

Special Factors Affecting Confidentiality Impact Determination: While the consequences of unauthorized disclosure of some financial sector oversight information would have only a limited