

April 2005

INFORMATION SECURITY

Improving Oversight of Access to Federal Systems and Data by Contractors Can Reduce Risk



G A O

Accountability * Integrity * Reliability

Contents

Letter

Results in Brief	1
Background	2
Federal Agencies Face a Range of Risks from Contractors and Other Users of Federal Data and Systems	4
Agencies Use Various Methods for Overseeing Contractor Security	10
Administration Efforts to Improve Information Security of Contractors Continue, but Challenges Remain	14
Conclusions	21
Recommendations for Executive Action	25
Agency Comments on Our Evaluation	26
	27

Appendixes

Appendix I: Objectives, Scope, and Methodology	29
Appendix II: Comments from the Department of Commerce	31
Appendix III: GAO Contact and Staff Acknowledgments	33
GAO Contact	33
Staff Acknowledgments	33

Tables

Table 1: Examples of Agency-Identified Risks to Federal Systems and Data Resulting from Reliance on Contractors	13
Table 2: The FAR Privacy or Security Safeguards Contract Language	15
Table 3: Number of Contractor Facilities and Operations Reported in Fiscal Year 2004	22

Figures

Figure 1: Federal Sources for Addressing Information Security Oversight of Contractor-Delivered IT Systems and Services	6
Figure 2: Major Agencies with Security Policies for Contractors, Privileged Users of Federal Data and Systems, and Contractor Security Oversight	18
Figure 3: Total Contractor Facilities and Number of Facilities Reviewed for 23 Federal Agencies in Fiscal Years 2002-2004	23

Abbreviations

CFO	chief financial officer
DOD	Department of Defense
FAR	Federal Acquisition Regulation
FISMA	Federal Information Security Management Act of 2002
GSA	General Services Administration
IT	information technology
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget

This is a work of the U.S. government and is not subject to copyright protection in the United States. It may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



United States Government Accountability Office
Washington, D.C. 20548

April 22, 2005

The Honorable Tom Davis
Chairman, Committee on Government Reform
House of Representatives

The Honorable Adam Putnam
House of Representatives

The federal government increasingly relies on information technology (IT) systems to provide essential services affecting the health, economy, and defense of the nation. To assist in providing these important services, the federal government relies extensively on contractors to provide IT services and systems. In addition to contractors that provide systems and services to the federal government, other organizations possess or use federal information or have access to federal information systems. These other organizations with privileged access to federal data and systems can include grantees, state and local governments, and research and educational institutions.

The Office of Management and Budget (OMB) cited contractor security as a governmentwide challenge in a 2001 information security report to Congress. Recognizing the need for agencies to have effective information security programs, Congress passed the Federal Information Security Management Act of 2002 (FISMA), which provides the overall framework for ensuring the effectiveness of information security controls that support federal operations and assets. FISMA requirements apply to all federal contractors and organizations or sources that possess or use federal information or that operate, use, or have access to federal information systems on behalf of an agency.

Our objectives were to (1) describe the information security risks associated with the federal government's reliance on contractor-provided IT systems and services and other users with privileged access to federal data and systems; (2) identify methods used by federal agencies to ensure security of information and information systems that are operated, used, or accessed by contractors and other users with privileged access to federal data; and (3) discuss steps the administration is taking to ensure implementation and oversight of security of information and information systems that are operated, used, or accessed by contractors and other users with privileged access to federal data and systems.

To accomplish our review, we surveyed the 24 Chief Financial Officers Act (CFO) agencies¹ regarding their policies and procedures for overseeing contractor security. We analyzed documentation submitted by the federal agencies and interviewed relevant officials in OMB, the General Services Administration (GSA), the Federal Acquisition Regulation Council, the National Institute of Standards and Technology (NIST), and private sector officials in the banking and finance industries. We conducted our work between August 2004 and March 2005 in accordance with generally accepted government auditing standards. Details of our objectives, scope, and methodology are included in appendix I.

Results in Brief

Contractors and users with privileged access to federal data and systems provide valuable services that contribute to the efficient functioning of the government, but a range of risks (including operational, strategic, and legal) must be managed effectively. Most agencies recognize risks to the confidentiality, integrity, and availability of their information and systems associated with the use of contractors and other users with privileged access to federal data and systems. For example, malicious code can be inserted into agency software and systems. In addition, agencies also reported specific risks when contractors develop software or perform work at off-site facilities. Federal agencies reported additional risks to their operations posed by other users with privileged access to federal data and systems, such as lack of controlled network connections, poor access controls, and the introduction of viruses and worms.²

Agencies use contracts, policies, and self-assessments for ensuring information security oversight of contractors; however, each of these

¹These 24 CFO departments and agencies are the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, Interior, Justice, Labor, State, Transportation, Treasury, Veterans Affairs, Environmental Protection Agency; General Services Administration; National Aeronautics and Space Administration; National Science Foundation; Nuclear Regulatory Commission; Office of Personnel Management; Small Business Administration; Social Security Administration; and U.S. Agency for International Development.

²A *virus* is a program that “infects” computer files, usually executable programs, by inserting a copy of itself into the file. These copies are usually executed when the infected file is loaded into memory, allowing the virus to infect other files. A virus requires human involvement (usually unwittingly) to propagate. A *worm* is an independent computer program that reproduces by copying itself from one system to another across a network. Unlike computer viruses, worms do not require human involvement to propagate.

methods has limitations and needs further strengthening. Most agencies reported using contract language to establish information security requirements for contractors. However, agency-provided contract language generally did not address key elements of FISMA, such as annual testing of controls. In addition, the majority of agencies reported having information security policies for contractors and almost two-thirds of the agencies reported having such policies for other users with privileged access to federal data. Yet our analysis of agency-provided policies found that only 5 agencies had established policies that specifically addressed information security oversight of contractor-provided systems. Finally, the majority of agencies reported using the NIST self-assessment tool to assess contractor security capabilities. However, only 10 reported using the tool to assess the security implemented by other users with privileged access to federal data.

The administration continues in its efforts to improve information security oversight of contractors, but challenges remain. For example, efforts to update the Federal Acquisition Regulation (FAR) to include the information security requirements of FISMA (which would be reflected in all relevant government contracts) have been under way since 2002, but are not yet complete. OMB continues to gather data about the number of agency systems, including those that are operated by contractors, and how many have been reviewed using a self-assessment tool. However, the data submitted showed that several agencies' chief information officers and inspectors general disagreed on the number of contractor or agency systems by as many as 100 systems or more. In addition, the data collected by OMB does not address other users with privileged access to federal data or the quality of the self assessments. Finally, NIST has developed guidance, parts of which are relevant to contractor security oversight. However, unified governmentwide guidance for overseeing information security of contractors and other users with privileged access to federal data and systems has not been issued.

We are making recommendations to the Director of OMB to ensure that (1) the FAR update efforts complement agency security management efforts required by FISMA; (2) federal agencies develop policies for information security oversight of contractors and other users with privileged access to federal data; and (3) agencies review the security of other users with privileged access to federal data and systems. Additionally, we are making recommendations to the Secretary of Commerce to develop a unified set of guidance to assist agencies in developing appropriate information security policies for managing risks related to contractors and other users with privileged access to federal data and systems.

In commenting on a draft of this report, OMB officials provided oral comments that generally agreed with the results of this report. Additionally, the Deputy Secretary of Commerce provided written comments that agreed with our findings and stated that the department is planning to develop a consolidated framework for contractor-related guidelines.

Background

The U.S. government is one of the largest users and acquirers of data, information, and supporting technology systems in the world, and plans to invest approximately \$65 billion annually on IT. These investments include the acquisition of IT services and systems from thousands of contractors.³ The ability to contract for technology services can allow an agency to obtain or offer enhanced services without the cost of owning the required technology or maintaining the human capital required to deploy and operate it. The systems and services provided by contractors include computer and telecommunication systems and services, as well as the testing, quality control, installation, and operation of computer equipment. Additionally, contractors provide services and systems to agencies by

- providing IT services and systems at agency facilities;
- providing IT services and systems on behalf of the agency at contractor facilities;
- providing IT services and systems to an agency via remote access; and
- developing or maintaining IT systems or software.

In its fiscal year 2001 report to Congress on federal government information security reform, OMB identified poor security oversight of contractor-provided IT systems and services as a common governmentwide challenge. In that report, OMB stated that IT contracts should include adequate security requirements, but that many agencies had reported no

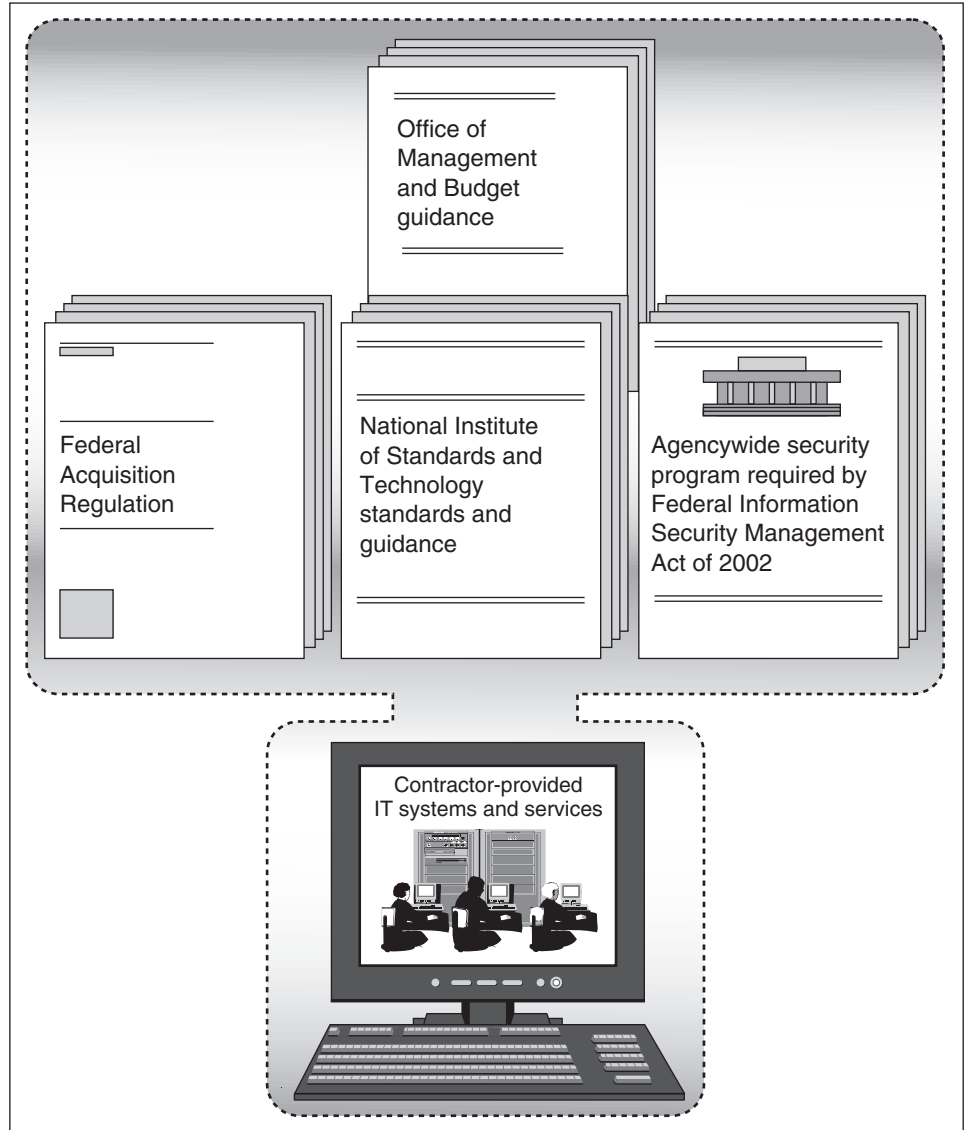
³Contractors are generally considered to be the primary entity with which a department or agency enters into an agreement. In this report, we use the term “contractor” when referring to both contractors and subcontractors. We refer to other organizations that possess or use federal information or have access to federal information systems—such as grantees, state and local governments, and research and educational institutions—as other users with privileged access to federal data and systems.

security controls in contracts or no verification that contractors fulfill any requirements that are in place.

**Federal Law and Policy
Address Planning and
Oversight for Information
Security**

Information security is an essential component of the acquisition, development, management, and oversight of IT systems and services delivered by contractors. When relying on contractors, a federal agency transfers operational responsibilities for performing one or more IT service(s) to one or more external providers. However, the overall responsibility and accountability for securing the information and systems remains with the federal agency (see fig. 1).

Figure 1: Federal Sources for Addressing Information Security Oversight of Contractor-Delivered IT Systems and Services



Sources: GAO (analysis), Art Explosion (clipart).

As depicted in figure 1, federal sources for addressing information security oversight of contractor-delivered IT systems and services are as follows

-
- FAR: emphasizes basic planning for the acquisition process;⁴
 - FISMA: requires an agencywide information security program that extends to contractors and other users with privileged access to federal data and systems;⁵ and
 - NIST standards and guidance and OMB guidance: assist agencies in establishing necessary security programs.

The FAR Emphasizes Planning and Includes Certain Information Security Requirements

The FAR emphasizes planning and includes certain specific information security requirements and provides the primary regulation for federal executive agencies in their acquisition of IT supplies and services with appropriated funds.

Additionally, in implementing federal privacy requirements, agencies are to ensure that contracts for the design, development, or operation of records systems using commercial IT services or support services include the following

- agency rules of conduct that the contractor and the contractor's employees shall be required to follow;
- a list of the anticipated threats and hazards that the contractor must guard against;
- a description of the safeguards that the contractor must specifically provide; and
- requirements for a program of government inspection during performance of the contract that will ensure the continued efficacy and efficiency of safeguards and the discovery and countering of new threats and hazards.

⁴48 C.F.R. Chapter 1.

⁵*Federal Information Security Management Act of 2002, Title III, E-Government Act of 2002*, Pub. L. No. 107-347 (Dec. 17, 2002).

The FAR requires agencies to ensure that IT contracts address privacy protections in accordance with the Privacy Act.⁶

FISMA Implementation Extends to Federal Contractors and Others

FISMA requires each agency to develop, document, and implement an agencywide information security program to protect information and information systems, including those provided or managed by another agency, contractor, or accessed by other users with privileged access to federal data. Specifically, this information security program is to include the following

- periodic assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information or information systems;
- risk-based policies and procedures that cost-effectively reduce information security risks to an acceptable level and ensure that information security is addressed throughout the life cycle of each information system;
- subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems;
- security awareness training for agency personnel, including contractors and other users of information systems that support the operations and assets of the agency;
- periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, performed with a frequency depending on risk, but no less than annually, and that includes testing of management, operational, and technical controls for every system identified in the agency's required inventory of major information systems;
- a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency;

⁶Privacy Act of 1974, Pub. L. No. 93-579, 5 U.S.C. 552a; FAR Subpart 24.1, 48 C.F.R. Subpart 24.1.

-
- procedures for detecting, reporting, and responding to security incidents; and
 - plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.

Federal agencies' implementation of FISMA requirements extends to contractors that are delivering IT systems and services and to other users of federal data and systems.⁷ In addition to these requirements, FISMA requires each agency to develop, maintain, and annually update an inventory of major information systems operated by the agency or that are under its control. This inventory is to include an identification of the interfaces between each system and all other systems or networks, including those operated by or under the control of contractors or other users with privileged access to federal data.

FISMA also requires each agency to have an annual independent evaluation of its information security program and practices, including control testing and compliance assessment. Evaluations of nonnational security systems are to be performed by the agency inspector general or by an independent external auditor. Furthermore, for nonnational security systems, FISMA requires NIST to develop (1) standards to be used by all agencies to categorize all of their information and information systems based on the objectives of providing appropriate levels of information security according to a range of risk levels; (2) guidelines recommending the types of information and information systems to be included in each category; and (3) minimum information security requirements for information and information systems in each category.

⁷In 2003, the Medicare Prescription Drug, Improvement, and Modernization Act (Pub. L. No. 108-173) was enacted. Section 912 of the act includes a provision requiring Medicare administrative contractors to implement a contractorwide information security program to provide information security for the operation and assets of the contractor for Medicare functions. Additionally, the information security program is required to meet certain requirements for information security programs already imposed on agencies and their data contractors by FISMA. Medicare administrative contractors are also required to undergo an annual independent testing and evaluation of their information security programs.

NIST Standards and Guidance and OMB Guidance Support FISMA Implementation

NIST standards and guidance and OMB guidance both support agency efforts to implement FISMA. NIST has issued a number of information security standards and guidance that is intended to promote the security of federal IT systems and services, such as its guidance on conducting risk assessments and on the format and content of security plans.⁸ In addition, as part of its statutory responsibilities under FISMA, NIST has issued standards and guidance that include consideration of security oversight of contractor-provided IT systems and services and other users with privileged access to federal data and systems.

In its fiscal year 2004 FISMA reporting guidance,⁹ OMB required federal agencies to use *NIST SP 800-26* or an equivalent assessment tool for agency annual information security reviews.¹⁰ The self assessments were also to be used to evaluate the security of contractor-provided IT systems and services. The self assessments provide a method for agency officials to determine the current status of their information security programs and, where necessary, to establish a target for improvement.

Federal Agencies Face a Range of Risks from Contractors and Other Users of Federal Data and Systems

Federal agencies face a range of risks from contractors and other users with privileged access to federal data and systems. Contractors that provide systems and services or other users with privileged access to federal data and systems can introduce risks to agency information and systems. Most agencies recognize the contractor-related risks, including those associated with contractor software development and off-site operations. Further, agencies view users with privileged access to federal systems and data as potential sources of risk.

⁸NIST, *Risk Management Guide for Information Technology Systems*, Special Publication 800-30 (Gaithersburg, Md.: July 2002) and *Guide for Developing Security Plans for Information Technology Systems*, Special Publication 800-18 (Gaithersburg, Md.: December 1998).

⁹OMB, *Fiscal Year 2004 Reporting Instructions for the Federal Information Security Management Act*, M-04-25(Washington, D.C.: Aug. 23, 2004).

¹⁰NIST, *Security Self-Assessment Guide for Information Technology Systems*, NIST Special Publication 800-26 (Gaithersburg, Md.: November 2001).

Contractors and Other Users of Federal Data and Systems Introduce Risks to Agencies

Contractors and other users with privileged access to federal data and systems can introduce information security risks to federal information and information systems that are sometimes difficult to quantify. Examples of these risks are as follows.

Strategic. Two basic strategic risks include management inexperience in overseeing contractor/other organization operations and the potential for inaccurate contractor/other organization information to negatively impact agency decisions. For example, inadequate management experience and expertise can impede an agency's ability to understand and control key risks. Additionally, inaccurate information from a contractor/other organization may prevent the leadership of an organization from having the necessary data to make well-informed strategic decisions.

Reputation. Errors, delays, system failures, or unauthorized disclosure of information may negatively impact how citizens, state and local governments, and other federal agencies view an agency and its services or mission.

Legal/Compliance. Federal agencies are required to ensure that their information security programs are being applied to systems and services that are being provided by contractors/other organizations and ensure compliance with laws such as privacy protections.

Implementation. Initiating a contractor relationship may require a complex transition of people, processes, hardware, software, and other assets from the agency to the provider or from one provider to another, all of which may introduce new risks.

Ownership/Dependence. An agency may ignore certain security issues due to "out of sight, out of mind" thinking, having delegated this concern to the provider. An agency may also become dependent on a particular contractor.

Operational. In addition to fraud or error, contractor or privileged access information security weaknesses could negatively impact agency operations, including delivering products; managing information; maintaining operations and transaction processing; customer service; systems development and support; and internal control processes.

Shared Environment. Contractors may use one system to service multiple clients and, as a result, this system-sharing may pose more risks than an in-

house environment. For example, sharing a common network or a processing environment, such as a general purpose server, across multiple clients can increase the likelihood of one organization having access to the sensitive information of another.

The risks identified can present complex challenges to federal agencies. Many of the complexities stem from risks related to people, processes, or technologies that, if not properly overseen or managed, can potentially harm an agency's operations, information, or systems.

Most Agencies Recognize Contractor-Related Risks to Information

Most agencies (17 of 24) reported that they recognize contractor risks to their information and information systems. These people, process, and technology risks can degrade or diminish the confidentiality, integrity, and availability of agency information systems or data. Examples of agency-identified risks are summarized in table 1.

Table 1: Examples of Agency-Identified Risks to Federal Systems and Data Resulting from Reliance on Contractors

Category	Risk description
People	Unauthorized personnel having physical access to agency IT resources (including systems, facilities, and data).
	Unauthorized personnel having electronic access to agency IT resources (including systems and data).
	Increased use of foreign nationals.
	Contractor or privileged users of federal data and systems who may not receive appropriate, periodic background investigations.
	Inadequate segregation of duties (e.g., software developer is the same individual who puts the software into production).
Processes	Failure by contractor or privileged users of federal data and systems to follow agency IT security requirements.
	Possible disclosure of agency-sensitive information to unauthorized individuals or entities.
	Lack of effective compliance monitoring of contractors performing work off-site or privileged users of federal data and systems.
	Contractor or privileged users of federal data and systems may have ineffective patch management processes.
Technology	Incorporation of unauthorized features in customized application software. For example, a third-party software developer has the potential to incorporate “back doors,” spyware, or malicious code into customized application software that could expose agency IT resources to unauthorized loss, damage, modification, or disclosure of data.
	Encryption technology may not meet federal standards.
	Intentional or unintentional introduction of viruses and worms.

Source: GAO analysis of federal agencies' survey response data.

Note: The various risks identified in table 1 could represent multiple risks (i.e. risks in one or more of the identified categories of people, processes and technology).

In addition to the risks identified in the table, agencies identified specific risks from contractor software development activities and off-site operations. These risks include the following

- a poor patch management process could impact federal operations, such as agency Web sites;
- the hosting infrastructure may not separate customer and company data; and
- the need for oversight at an off-site facility.

Without proper controls, the risks associated with software development and work performed off site could be very damaging to federal information and systems. For example, loss of confidentiality, integrity, or availability of data can disrupt federal operations and services and may impede the ability to ensure the performance of mission-critical functions.

Agencies Assess Users with Privileged Access to Federal Data and Systems as Potential Risks

Many agencies reported their risks from other users with privileged access to federal data and systems. Seventeen agencies indicated that they assess the risks posed by other users with privileged access to federal data and systems. Agency-identified risks included

- lack of controls on network connections;
- unauthorized use or release of information, such as grantee information being revealed to another grantee;
- malicious activity that introduces viruses and worms; and
- poor electronic access controls that could permit customer passwords to be compromised and exploited by identity theft.

Of the remaining 7 agencies, 5 indicated that other users do not possess or use their data and systems; 1 indicated that it had not assessed risks of other users with privileged access; and the other agency did not respond regarding whether they had assessed risks of other users with privileged access to federal data and systems.

Agencies Use Various Methods for Overseeing Contractor Security

Federal agencies report using three primary methods for overseeing the information security of contractors

- using contract language to establish information security requirements for contractors;
- having information security policies for contractors and other users with privileged access to federal data; and
- using NIST self-assessment tools to assess contractor security capabilities and assess the security implemented by other users with privileged access to federal data.

These methods can be leveraged for effective agency oversight of contractors and privileged users for federal systems and data. However when not properly implemented, each of these methods has limitations.

Agencies Use Contract Language to Establish Information Security Requirements

Most agencies report using contract language to establish information security requirements for contractors. The FAR requires that agencies use specific contract language related to privacy or security safeguards. Table 2 contains an example of FAR-provided language for agencies to include in their IT contracts.

Table 2: The FAR Privacy or Security Safeguards Contract Language

- (a) The Contractor shall not publish or disclose in any manner, without the Contracting Officer's written consent, the details of any safeguards either designed or developed by the Contractor under this contract or otherwise provided by the Government.
- (b) To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of Government data, the Contractor shall afford the Government access to the Contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases.
- (c) If new or unanticipated threats or hazards are discovered by either the Government or the Contractor, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party.

Source: Federal Acquisition Regulation 52.239-1.

This FAR language helps ensure that federal agencies can maintain access to contractor facilities in order to perform security oversight functions. However, this language does not address all aspects of security. For example, the clause in table 2 does not apply to subcontractors. By not including subcontractors within specific information security requirements, agencies can be introducing significant risks without a contractual tool with which to manage them.

More importantly, the FAR has not been amended to reflect the requirements of the FISMA. As a result, the language in the FAR does not reflect key FISMA requirements, including

- periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices performed with a frequency depending on risk, but not less than annually, and including testing of management, operational, and technical controls for every system

identified in the agency's required inventory of major information systems;

- a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency;
- procedures for detecting, reporting, and responding to security incidents; and
- plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.

The FAR provides, however, that this contract language only needs to be “substantially the same” as standard FAR clauses and agencies, therefore, have the flexibility to modify it to address FISMA requirements. Additionally, agencies are authorized to include in their agency FAR supplements, regulations, and clauses that supplement FAR policies and procedures or satisfy specific needs of the agency.¹¹ Agency FAR supplements, accordingly, could include additional language to address the requirements of FISMA.

However, although some agency FAR supplements include requirements related to IT security that are not in the FAR, no agency has made a comprehensive effort to revise its FAR supplement to reflect FISMA.

The 2003 NIST SP 800-35¹² stresses the importance of establishing security requirements with external parties in formal contracts. However, by not establishing clear security requirements in contracts, agencies may not be able to ensure that their agency information is secured in accordance with FISMA.

¹¹FAR Subpart 1.3; 48 C.F.R. Subpart 1.3.

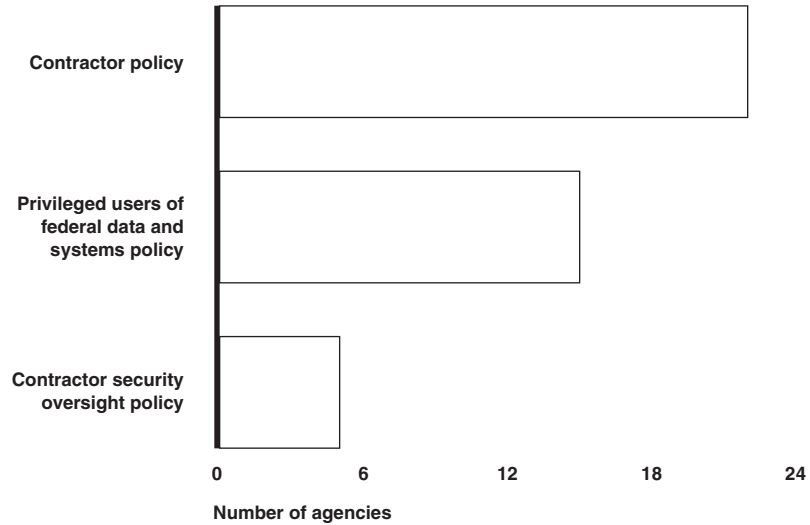
¹²NIST, *Guide to Information Technology Services*, Special Publication 800-35 (Gaithersburg, Md.: October 2003).

Most Agencies Have Information Security Policies for Contractors, but Few Policies Provide for Oversight Capabilities

Although most agencies reported having written policies that addressed information security for contractor-provided IT services and systems and for other users with privileged access to federal data and systems, few established specific policies for overseeing the information security practices of contractors to ensure compliance with contract requirements and agency information security policies. As figure 2 illustrates, 22 of the surveyed agencies reported having information security policies for contractors, and 15 reported having policies for other users with privileged access to federal data and systems. However, the majority of agencies addressed contractors and other users with privileged access to federal information and systems within the general scope of their agency policy, and did not define information security oversight requirements. For example, agency policies did not describe oversight methods; the frequency of reviews or assessments; key management controls to mitigate unauthorized disclosure of information; physical/logical access controls; or the introduction of unauthorized features. Further, most of the agencies did not have policies or provide guidance on key areas, including control of agency data in an off-site facility or requirements for interconnection security agreements.¹³

¹³An interconnection security agreement documents specific technical and security requirements for connecting IT systems from different organizations, such as between a federal agency and a contractor or between a federal agency and other users with privileged access to federal data and systems.

Figure 2: Major Agencies with Security Policies for Contractors, Privileged Users of Federal Data and Systems, and Contractor Security Oversight



Source: GAO analysis based on agency data.

However, we identified only 5 agencies that had established specific policies addressing contractor information security oversight. While the five agency policies reflected a broad range of maturity levels, they included many of the following elements

- establishing procedures for contractor information security oversight;
- assigning roles and responsibilities;
- creating specific audit plans for systems and facilities;
- describing interconnection security agreements;
- creating requirements for agency information that will be secured at contractor facilities—including storing, processing, and transmitting on contractor systems, background checks, and facility security; and
- requiring agency officials to conduct reviews to ensure that IT security requirements were being enforced.

By establishing oversight policies that address these elements, agencies can more consistently oversee contractor security and ensure that contractors and other users with privileged access to federal systems and data comply with agency security requirements. However, without such policies, oversight efforts can be impeded.

In fiscal years 2003 and 2004, many agency inspectors general cited the lack of agency policies and guidance regarding how agency program managers or organizational components should conduct oversight of contractor operations as problematic. Three different agency inspectors general reported the following

- Agency policies and procedures did not provide organizational components with guidance on conducting reviews of their contractor-provided services. Further, there was little evidence that components are ensuring that contractor-provided services are secure and comply with agency security policy.
- Agency program officials had not ensured that (1) adequate security of contractor-provided services, including not identifying the full range of services provided and that (2) oversight processes and procedures for ensuring secure operations had not been defined or implemented.
- Agency officials were not using adequate methods to ensure that contractor security met the requirements of FISMA, OMB, and NIST guidelines after reviewing the access controls, security clearances, and security awareness training for contractors that provide network administration, systems development, and systems administration.

Without appropriate policies and guidance, agencies may not be able to effectively and efficiently assess the security of contractor operations or that of other users with privileged access to federal data and systems. For example, without specific oversight policies establishing when and how agencies will review contractor-operated systems, officials responsible for the systems may not be taking sufficient action to ensure that security requirements are being met. Further, information system controls needed to ensure secure operations may not be tested on regular intervals. As a result, agencies may not be able to protect federal information in accordance with FISMA.

Agencies Use Self-Assessment Tool to Review Contractor Security, but Its Oversight Value May Be Limited

The majority of agencies reported using a self-assessment tool to review contractor information security, but the oversight value may be limited. NIST's self-assessment guide states that self-assessments provide a method for agency officials to determine the current status of their information security programs and, where necessary, to establish a target for improvement. NIST SP 800-26 structures the questionnaire by management, operational, and technical controls. The section on technical controls does not require testing of those controls as part of the self-assessment, but instead relies on documentation. In response to our survey, 22 agencies reported using NIST SP 800-26 to assess contractors providing IT services and systems and 2 agencies reported not using this assessment tool.

While most agencies reported using NIST SP 800-26, the self-assessment tool may have limited value in overseeing contractor information security. For example, by relying on a contractor's self assessment, an agency official may not obtain a clear understanding of the effectiveness of security controls or be assured of the validity of the responses without independent testing. Further, the agency chief information officer or inspector general may have trouble conducting an analysis or review of the self assessment if there is not sufficient documentation.

As an example of the self-assessment challenges, one agency inspector general found significant problems with the agency's self assessment. The inspector general noted that, after reviewing a sample of the agency's NIST SP 800-26 self assessments, (1) security weaknesses had not been properly defined, (2) variations existed between inspector general and agency scoring on the NIST SP 800-26 reviews, and (3) the agency did not verify the results of self assessments.

Further, the lack of information security requirements established in contracts and the absence of agency oversight policies may diminish the efforts of reviewers using NIST SP 800-26 because they may not be able to refer to clear criteria with which to assess systems' security. As a result, agencies may not obtain an accurate status of the security of contractor-provided systems and services.

Many Agencies Do Not Review Other Users with Privileged Access to Federal Data and Systems

In August 2004, OMB mandated the use of NIST SP 800-26 for agency annual system reviews. However, in response to our survey, only 10 agencies reported using NIST SP 800-26 to assess other users with privileged access to federal data and systems that have connectivity to agency networks. By not assessing and testing the security controls of

other users with privileged access to federal data, agencies reported that they are at increased risk of losing control of network connections, experiencing unauthorized use of information, such as grantee information being revealed to another grantee, and malicious activity that introduces viruses and worms.

Administration Efforts to Improve Information Security of Contractors Continue, but Challenges Remain

The administration is making efforts to improve information security over contractors, but challenges remain. For example, the information security requirements in FAR are being revised and OMB continues to gather data from the agencies about the number of contractor facilities reviewed by agencies. Additionally, NIST has issued guidance, parts of which address some contractor security issues.

Federal Acquisition Regulation Is Being Updated to Modernize IT Requirements

In response to the administration's plans to update FAR, officials at the FAR Council stated that the acquisition regulation was being updated to address information security requirements of contractor-provided systems and services. Officials further explained that the administration had been working on updating the FAR language since 2002 when FISMA was enacted. According to the FAR Council officials, the council had completed the majority of its work in December 2004. As of March 2005, the FAR amendments were undergoing legal review.

OMB Collects Data on Agency Information Security Oversight of Contractors, but Effectiveness of Agency Efforts Is Unclear

Through its FISMA reporting requirements, OMB continues to gather information about agency oversight of contractors, but understanding the effectiveness of agency efforts based on the collected data is unclear. On an annual basis, OMB collects information from the agencies about

- the total number of agency systems, including whether the chief information officer and the inspectors general agree on the number of systems identified and
- the number of contractor facilities and operations identified and reviewed using NIST SP 800-26 or an equivalent methodology.

The fiscal year 2004 FISMA submissions revealed significant discrepancies in the responses from the agency and the inspector general. For example, as shown in table 3, the number of systems reported as being agency

systems or contractor systems varied significantly among the chief information officers and the inspectors general at four agencies. Without a clear understanding of who has operational control of a system, agencies cannot ensure that the appropriate oversight and security controls are being implemented in accordance with agency policy.

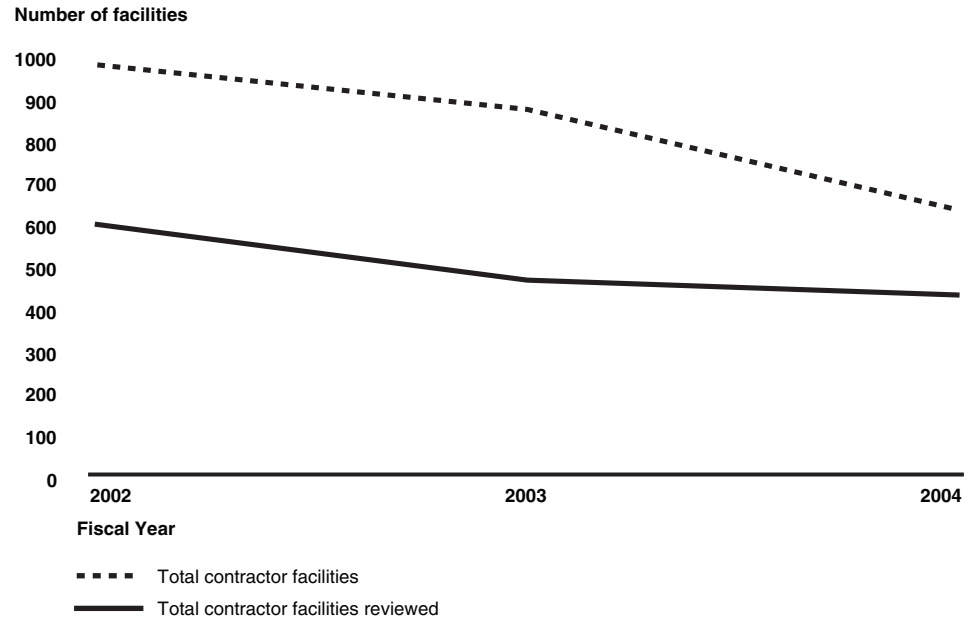
Table 3: Number of Contractor Facilities and Operations Reported in Fiscal Year 2004

Agency	Agency/chief information officers total	Inspectors general total
Agency A	61	13
Agency B	11	65
Agency C	4	111
Agency D	20	5

Source: Fiscal year 2004 agency chief information officer and inspectors general FISMA submissions to OMB.

Over the past 3 years, there has been a decline in both the number of contractor facilities identified by the agencies and the number of facilities reviewed by the agencies. Figure 3 depicts this trend in 23 of the major agencies.

Figure 3: Total Contractor Facilities and Number of Facilities Reviewed for 23 Federal Agencies in Fiscal Years 2002-2004



Source: Agency/GISRA/FISMA.

Note: The Department of Defense contractor facilities and number of facilities reviewed are not reflected in the figure because this information was not available for 2002. However, in 2003, the DOD reported identifying 4,716 contractor facilities and reviewing 4,000 facilities, while in 2004, the department inventoried 4,686 and reviewed 3,961 facilities.

The disagreement between agency chief information officers and inspectors general about whether systems are deemed to be agency systems or contractor systems can impede effective and efficient information security oversight efforts. In some cases, it may even result in systems not being reviewed. By not performing reviews of contractor-operated facilities, agencies cannot ensure that their information is being protected in accordance with FISMA and, as a result, federal operations and data can be at risk.

The data gathered from the agencies on the number of contractor systems identified and reviewed do not provide an accurate measure of the effectiveness of agency information security oversight of contractors. However, additional data about the contracts, policies, and self assessments could provide a better measure of effectiveness. For example, asking inspectors general to determine

-
- what portion of the contractor systems identified by the agencies have specific IT security language that addresses key FISMA elements;
 - if the agency information security policies provide specific oversight policies for contractors and privileged users of federal systems and data; and
 - whether the required NIST SP 800-26 assessments of contractor systems were completed by the agency, the contractor, or an independent entity.

Finally, annual agency reports required by FISMA do not address security related to other users with privileged access to federal data. There is not a clear governmentwide understanding of how agencies are addressing the various challenges and identified risks related to other users with privileged access. As previously discussed, agencies have not developed policies or reviewed the controls necessary to ensure that these users of federal data do not place agencies' information and systems at risk of compromise. As a result, federal agencies that lack appropriate controls and oversight can be exposing their information and systems to additional risks from privileged users who might introduce malicious code, disclose unauthorized information, or lack controls to secure their network interfaces with the agency systems.

Unified Federal Guidance Could Assist Agencies

No single federal guide exists for federal agencies to rely on when addressing information security over contractors. FISMA requirements apply to all federal contractors and organizations or sources that possess or use federal information or that operate, use, or have access to federal information systems on behalf of an agency. In support of FISMA implementation, NIST has issued a number of information security products intended to improve federal IT systems.

However, in the absence of a single, comprehensive guide to assist in the development of policies, agencies must refer to portions of several different documents that address elements related to contractor information security oversight. For example, in 2005, NIST published *Recommended Security Controls for Federal Information Systems*,¹⁴ which refers to portions of the following documents that can be used by

¹⁴NIST, *Recommended Security Controls for Federal Information Systems*, Special Publication 800-53 (Gaithersburg, Md.: February 2005).

agencies to address some of the challenges related to information security oversight of contractors

- *SP 800-18* states that agencies may require compliance with the guide as part of contract requirements;
- *SP 800-35* lists in its appendices sample acquisition language that is appropriate for inclusion into IT security service statements of work;
- *SP 800-47* discusses, in brief, the development of non-disclosure agreements for contractors when determining interconnection requirements; and
- *800-64* gives examples of contract clauses that can be used to help establish clear lines of authority and responsibility.

In February 2005, NIST released the Federal Information Processing Standard 201 entitled *Personal Identity Verification of Federal Employees and Contractors*. This standard was developed in response to Homeland Security Presidential Directive 12 and is intended to improve the identification and authentication of federal employees and contractors for access to federal facilities and information systems. This standard helps to address the risk of contractors gaining unauthorized physical or electronic access to federal information.

Unified guidance on addressing the information security oversight of contractors and privileged users of federal systems and data could assist agencies in developing effective programs to ensure compliance with agency policy. However, without clear guidance on how to develop effective information security oversight of contractors and users with privileged access to federal systems and data, federal agencies may not develop sufficient policies to address the range of risks posed by contractors and key users. As a result, federal information and operations can be placed at undue risk.

Conclusions

Contractors provide valuable services that contribute to the efficient functioning of the government, but a range of risks from contractors and other users with privileged access to federal data and systems must be managed effectively. Contracts, policies, and security self-assessments can be leveraged as valuable oversight tools for federal agencies in managing oversight of contractors and other users. However, when not properly

implemented, each of these methods has limitations. For example, many agencies are not incorporating FISMA requirements into their contract language; accordingly, their strongest tool for establishing information security requirements is limited. Additionally, many agencies have not defined specific oversight policies for contractors and other users with privileged access to federal data. Without clearly defined information security oversight policies, agencies may be accepting significant risk to their information and systems from both contractors and other users with privileged access without having the appropriate controls to mitigate the risks. Finally, agency reliance on self-assessment tools may not provide them with the appropriate tools to ensure the security of their information.

To address these complex challenges, a variety of administration efforts have been started to further enhance federal agencies' efforts to improve information security oversight of contractors, but challenges remain. For example, the effort to update FAR guidance has not been completed. In addition, continuing OMB FISMA oversight reveals challenges in contractor oversight. Finally, if agencies lack unified guidance to assist them in creating appropriate information security oversight policies for contractors and other users with privileged access to federal data and systems, federal agencies may not be able to effectively protect their information.

Recommendations for Executive Action

To ensure that agencies are developing the appropriate information security oversight capabilities for contractors and other users with privileged access to federal data and systems, we recommend, in accordance with FISMA, that the Director of OMB ensure that the following two actions take place.

- Efforts to update FAR are completed expeditiously and that such efforts require agency security management efforts required by FISMA, including
 - periodic testing and evaluation of management, operational, and technical controls;
 - a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies and procedures;

-
- procedures for detecting, reporting, and responding to security incidents; and
 - plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.
 - Federal agencies develop policies for ensuring information security of contractors and other users with privileged access to federal data, including
 - establishing procedures for contractor information security oversight;
 - assigning roles and responsibilities;
 - creating specific audit plans for systems and facilities;
 - describing interconnection security agreements;
 - creating requirements for agency information that will be secured at contractor facilities including storing, processing, transmitting on contractor systems, background checks, and facility security; and
 - requiring agency officials to conduct reviews to ensure that IT security requirements are being enforced.

To assist agencies in managing the risks related to contractors and other users with privileged access to federal data and systems, we recommend that the Secretary of Commerce develop a unified set of guidance for developing appropriate information security policies.

Agency Comments on Our Evaluation

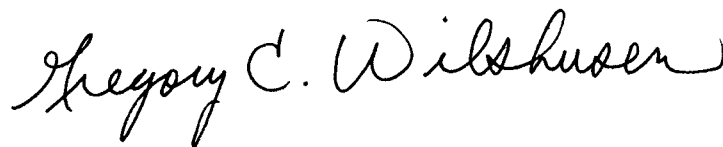
We provided a draft of this report to OMB and the Department of Commerce for their official review and comment. OMB General Counsel provided oral comments on the report, which have been incorporated as appropriate. OMB generally agreed with the report findings and conclusions. OMB officials told us that, as part of the capital asset plan and business case development process, agencies are required to answer several information security oversight questions related to contractor-provided IT systems and services. These questions provide OMB important information when assessing the business case for funding. Further, OMB

stated that their efforts to enhance oversight of contractors includes requiring that the 25 E-Government initiatives be independently reviewed to determine compliance with IT security requirements. OMB did not disagree with the overall recommendations and recognized the need for further agency action to address contractor security oversight.

In written comments, which are reprinted in appendix II, the Deputy Secretary of the Department of Commerce acknowledged the accuracy of the report. In regard to our recommendation, Commerce stated that NIST recognizes the importance of providing guidance to assist agencies in ensuring that security requirements are applied by contractors. Additionally, NIST has developed publications that can be used for contractors and are focused on acquisition, assessments, controls, and the system development life cycle. Commerce agreed that through NIST, it would develop a strategy to build a framework for a consolidated delivery of contractor related-guidelines.

As agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. At that time, we will send copies of this report to interested congressional committees; the Director, Office of Management and Budget; and the Secretary, Department of Commerce. We will also make copies available to others upon request. In addition, the report will be available at no charge on the GAO Web site at <http://www.gao.gov>.

If you or any of your staff have any questions concerning this report, please contact me at (202) 512-3317. I can also be reached by e-mail at wilshuseng@gao.gov. Other contacts and key contributors to this report are listed in appendix III.



Gregory C. Wilshusen
Director, Information Security Issues

Objectives, Scope, and Methodology

The objectives of our review were to

- Describe the information security risks associated with the federal government's reliance on contractors providing information technology systems and services and other users with privileged access to federal data and systems federal information or access federal information systems.
- Identify methods used by federal agencies to ensure security of information and information systems that are operated, used, or accessed by contractors and other users with privileged access to federal data.
- Discuss what steps the administration is taking to ensure implementation and oversight of security of information and information systems that are operated, used, or accessed by contractors and other users with privileged access to federal data.

To describe the information security risks associated with the federal government's reliance on contractors and other organizations, we analyzed existing federal regulations, laws, and guidelines such as the Federal Acquisition Regulation (FAR); Federal Information Security Management Act of 2002 (FISMA); and National Institute of Standards and Technology (NIST) guidance. In addition, we interviewed federal and private-sector officials regarding the policies and procedures for overseeing contractor security. We then developed a series of questions that were incorporated into a Web-based survey instrument. We pretested our survey instrument at one federal department and one federal independent agency. We also met with Office of Management and Budget (OMB) officials to discuss OMB's role in ensuring the security of contractor-provided systems and services. For each agency to be surveyed, we identified the office of the chief information officer, notified each office of our work, and, via e-mail, distributed a link to each office. All 24 agencies responded to our survey. We did not verify the accuracy of the agencies' responses; however, we reviewed supporting documentation that agencies provided to validate their responses. We contacted agency officials when necessary for follow-up.

Although this was not a sample survey and, therefore, there were no sampling errors, conducting any survey may introduce errors, commonly referred to as nonsampling errors. For example, difficulties in how a particular question is interpreted, in the sources of information that are

available to respondents, or in how the data are entered into a database or were analyzed can introduce unwanted variability into the survey results. We took steps in the development of the survey instrument, the data collection, and the data analysis to minimize these nonsampling errors. For example, a survey specialist designed the survey instrument in collaboration with GAO staff with subject-matter expertise. Then, as previously stated, it was pretested to ensure that the questions were relevant, clearly stated, and easy to comprehend. When the data were analyzed, a second, independent analyst checked all computer programs. Because this was a Web-based survey, respondents entered their answers directly into the electronic questionnaire. This eliminated the need to have the data keyed into a database, thus removing an additional potential source of error.

To identify methods used by federal agencies to ensure security of contractor-provided systems and services, we interviewed the FAR Council, OMB, and NIST officials to discuss their guidelines and other tools available to agencies. In addition, questions regarding agency policy, agency use of oversight guidelines, acquisition process, and personnel/background checks, security requirements, and contract language were included in the survey we sent to the 24 Chief Financial Officer's Act agencies. We did not verify the accuracy of the agencies' responses; however, we reviewed supporting documentation that agencies provided to validate their responses. We contacted agency officials when necessary for follow-up.

Finally, to determine what steps the administration is taking to ensure implementation and oversight of security of contractors and other users with privileged access that operate, use, or access federal information systems on behalf of an agency, we interviewed FAR Council, OMB, and NIST officials regarding the policies and procedures for overseeing contractor security. We also reviewed annual chief information officer and inspectors general FISMA reports to assess progress made in meeting FISMA requirements related to contractor security.

We conducted our work in Washington, D.C., from August 2004 through March 2005 in accordance with generally accepted government auditing standards.

Comments from the Department of Commerce



THE DEPUTY SECRETARY OF COMMERCE
Washington, D.C. 20230

April 19, 2005

Mr. Gregory Wilshusen
Director, Information Security Issues
United States Government Accountability Office
Washington, DC 20548

Dear Mr. Wilshusen:

I enclose the Department of Commerce's comments on Government Accountability Office (GAO) proposed report entitled Information Security: Improving Oversight of Access to Federal Systems and Data by Contractors Can Reduce Risk (GAO-05-362). Thank you for the opportunity to review the report. I commend the GAO for this study on the issue of improving information security oversight of contractors.

We recognize the need to develop cohesive government-wide guidance to assist agencies in developing appropriate information security policies for addressing contractors and other users with privileged access to federal data and systems. The National Institute of Standards and Technology (NIST) has developed a set of publications for acquisition, self-assessment, and controls that should be applied in developing information systems. In addition, NIST has recently developed a road map which maps NIST publications to the various phases of the system development life cycle. In support of the GAO proposed recommendation, NIST will extend its efforts to develop a strategy to build the necessary framework for a more consolidated delivery of the contractor related guidelines.

Again, thank you for the opportunity to comment on this draft report.

Sincerely,

A handwritten signature in black ink, appearing to read "Theodore W. Kassinger", is written in a cursive style.

Theodore W. Kassinger

Enclosure

**Comments on
Government Accountability Office (GAO) Report entitled “Information Security: Improving
Oversight of Access to Federal Systems and Data by Contractors Can Reduce Risk”
made by the
National Institute of Standards and Technology (NIST), Department of Commerce**

The GAO team should be commended for the study. The report provides a thorough assessment of the information security risks associated with the Federal Government’s reliance on contractor-provided IT systems and services and other users with privileged access to federal data and systems. Furthermore, it identifies current methods employed by federal agencies to avoid these risks, and provides recommendations to improve information security oversight for contractors.

NIST has reviewed the report and has noted no major errors or omissions. The report identified one major recommendation -- that the Secretary of Commerce develop a unified set of guidance for developing appropriate information security guidance related to contracting.

NIST recognizes the importance of providing guidance to assist agencies in ensuring that the appropriate security requirements are applied to contractors. We had previously developed a three-volume set of special publications (SP) specifically focused on acquisition (SP800-64, SP800-35, and SP800-36). In addition, SP 800-26, the NIST self-assessment tool, can be used for contractor assessments. Most recently, NIST published SP800-53 which defines in great detail the controls that should be applied in developing information systems. This document can be used to derive security requirements for systems being developed by contractors.
(<http://csrc.nist.gov/publications/nistpubs/index.html>)

Further, recognizing the need to provide one consolidated road map to the numerous NIST publications, which can be applied throughout the system development life cycle (SDLC), we recently published a reference which maps all of the NIST guidance to the various phases of the SDLC. It can be used by contractors to identify the appropriate references based on scope and focus of specific contract tasking.
(http://csrc.nist.gov/SDLCinfosec/SDLC_brochure_Aug04.pdf)

The above strategy has allowed NIST to develop information security publications in focused areas with the sufficient detail required to be useful.

To support the GAO proposed recommendation, NIST will extend its efforts to develop a strategy to build the necessary framework for a more consolidated delivery of the contractor-related guidelines.

GAO Contact and Staff Acknowledgments

GAO Contact

J. Paul Nicholas, Assistant Director, (202) 512-4457,
nicholasj@gao.gov

Staff Acknowledgments

In addition to the individual named above, key contributors to this report included Neil Doherty, Nancy Glover, Stuart Kaufman, Anjalique Lawrence, Nnaemeka Okonkwo, and Kevin Secrest.

GAO's Mission

The Government Accountability Office, the audit, evaluation and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "Subscribe to Updates."

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are \$2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm

E-mail: fraudnet@gao.gov

Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Gloria Jarmon, Managing Director, JarmonG@gao.gov (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, D.C. 20548

Public Affairs

Paul Anderson, Managing Director, AndersonP1@gao.gov (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, D.C. 20548

Appendix III
GAO Contact and Staff Acknowledgments
