September 2010

CONTRACTOR INTEGRITY

Stronger Safeguards Needed for Contractor Access to Sensitive Information

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-10-693, a report to the Chairman, Subcommittee on Federal Financial Management, Government Information, Federal Services, and International Security, Committee on Homeland Security and Governmental Affairs, U.S. Senate

Why GAO Did This Study

In performing agency tasks, contractor employees often require access to sensitive information that must be protected from unauthorized disclosure or misuse. This report assesses the (1) extent to which agency guidance and contracts contain safeguards for contractor access to sensitive information, and (2) adequacy of governmentwide guidance on how agencies are to safeguard sensitive information to which contractors may have access. To conduct this work, GAO identified key attributes involving sensitive-information safeguards, analyzed guidance and met with officials at three agencies selected for their extensive reliance on contractor employees, analyzed 42 of their contract actions for services potentially requiring contractor access to sensitive information, and analyzed the Federal Acquisition Regulation (FAR) and pending FAR changes regarding governmentwide guidance on contractor safeguards for access to sensitive information.

What GAO Recommends

GAO recommends that the Office of Federal Procurement Policy (OFPP) ensure pending changes to the FAR address two additional safeguards for contractor access to sensitive information: the use of nondisclosure agreements and prompt notification of unauthorized disclosure or misuse of sensitive information. In oral comments, OFPP agreed with the recommendations. DHS also concurred with the recommendations, while DOD and HHS had no comment.

View GAO-10-693 or key components.
For more information, contact John Needham at (202) 512-4841 or needhamjk1@gao.gov.

What GAO Found

GAO's analysis of guidance and contract actions at three agencies found areas where sensitive information is not fully safeguarded and thus may remain at risk of unauthorized disclosure or misuse. The Departments of Defense (DOD), Homeland Security (DHS), and Health and Human Services (HHS) have all supplemented the FAR and developed some guidance and standard contract provisions, but the safeguards available in DOD's and HHS's guidance do not always protect all relevant types of sensitive information contractors may access during contract performance (examples of some types of sensitive information contractors may access are listed below). Also, DOD's, DHS's, and HHS's supplemental FAR guidance do not specify contractor responsibilities for prompt notification to the agency if unauthorized disclosure or misuse occurs. Almost half of the 42 contract actions analyzed lacked clauses or provisions that safeguarded against disclosure and inappropriate use of all potential types of sensitive information that contractors might access during contract performance. Additionally, DOD and HHS lack guidance on the use of nondisclosure agreements, while DHS has found that these help accountability by informing contractors of their responsibilities to safeguard confidentiality and appropriate use and the potential consequences they face from violations.

There have been numerous recommendations for improved governmentwide guidance and contract provisions in the FAR, such as prohibiting certain types of contractor personnel from using sensitive information for personal gain. To address some of these areas, regulatory changes are pending to develop standardized approaches and contract clauses in the FAR that agencies could use to safeguard sensitive information, rather than developing such safeguards individually. However, similarly to issues identified in agency guidance, GAO found two key areas the FAR does not yet address. These include (1) agency use of nondisclosure agreements as a condition of contractor access to sensitive information, and (2) the need to establish clear requirements for contractors to promptly notify agencies of unauthorized disclosure and misuse of sensitive information. The ongoing rulemaking process provides an opportunity to address the need for additional FAR guidance in both areas.

Examples of Sensitive Information

Type of information	Examples
Personal	• Name • Social Security number • Date and place of birth • Patient health and medical information
Business proprietary	• Trade secrets • Manufacturing processes, operations, or techniques • Amount or source of any profits, losses, or expenditures.
Agency sensitive	• Security management information • Predecisional planning and budgeting documents • Continuity-of-operations information

Source: GAO analysis.