1837.203-70 Providing contractors access to sensitive information.

(a)

(1) As used in this subpart, “sensitive information” refers to information that the contractor has developed at private expense or that the Government has generated that qualifies for an exception to the Freedom of Information Act, which is not currently in the public domain, may embody trade secrets or commercial or financial information, and may be sensitive or privileged, the disclosure of which is likely to have either of the following effects: To impair the Government's ability to obtain this type of information in the future; or to cause substantial harm to the competitive position of the person from whom the information was obtained. The term is not intended to resemble the markings of national security documents as in sensitive-secret-top secret.

(2) As used in this subpart, “requiring organization” refers to the NASA organizational element or activity that requires specified services to be provided.

(3) As used in this subpart, “service provider” refers to the service contractor that receives sensitive information from NASA to provide services to the requiring organization.

(b)

(1) To support management activities and administrative functions, NASA relies on numerous service providers. These contractors may require access to sensitive information in the Government's possession, which may be entitled to protection from unauthorized use or disclosure.

(2) As an initial step, the requiring organization shall identify when needed services may entail access to sensitive information and shall determine whether providing access is necessary for accomplishing the Agency's mission. The requiring organization shall review any service provider requests for access to information to determine whether the access is necessary and whether the information requested is considered “sensitive” as defined in paragraph (a)(1) of this section.

(c) When the requiring organization determines that providing specified services will entail access to sensitive information, the solicitation shall require each potential service provider to submit with its proposal a preliminary analysis of possible organizational conflicts of interest that might flow from the award of a contract. After selection, or whenever it becomes clear that performance will necessitate access to sensitive information, the service provider must submit a comprehensive organizational conflicts of interest avoidance plan.

(d) This comprehensive plan shall incorporate any previous studies performed, shall thoroughly analyze all organizational conflicts of interest that might arise because the service provider has access to other companies' sensitive information, and shall establish specific methods to control, mitigate, or eliminate all problems identified. The contracting officer, with advice from Center counsel, shall review the plan for completeness and identify to the service provider substantive weaknesses and omissions for necessary correction. Once the service provider has corrected the substantive weaknesses and omissions, the contracting officer shall incorporate the revised plan into the contract, as a compliance document.

(e) If the service provider will be operating an information technology system for NASA that contains

sensitive information, the operating contract shall include the clause at 1852.204–76, Security Requirements for Unclassified Information Technology Resources, which requires the implementation of an Information Technology Security Plan to protect information processed, stored, or transmitted from unauthorized access, alteration, disclosure, or use.

(f) NASA will monitor performance to assure any service provider that requires access to sensitive information follows the steps outlined in the clause at 1852.237–72, Access to Sensitive Information, to protect the information from unauthorized use or disclosure.

Parent topic: Subpart 1837.2—Advisory and Assistance Services