■ 55. Appendix F to Chapter 2 is amended in Part 1, Section F–104, as follows:
■ a. In paragraph (a)(5)(i) introductory text by removing ''*Continental United States*'' and adding in its place ''*Contiguous United States*''; and
■ b. In paragraph (a)(5)(ii), in the first sentence, by removing ''continental U.S.'' and adding in its place ''contiguous United States''.

[FR Doc. 05–12100 Filed 6–20–05; 8:45 am]

BILLING CODE 5001–08–P

DEPARTMENT OF DEFENSE

48 CFR Part 252

Defense Federal Acquisition Regulation Supplement; Technical Amendments

AGENCY: Department of Defense (DoD).

ACTION: Final rule.

SUMMARY: DoD is making technical amendments to a Defense Federal Acquisition Regulation Supplement clause addressing unique identification and valuation of items delivered under DoD contracts. The amendments clarify cross-references and correct an Internet address.

DATES: Effective June 21, 2005.

FOR FURTHER INFORMATION CONTACT: Ms. Michele Peterson, Defense Acquisition Regulations System, OUSD(AT&L)DPAP(DAR), IMD 3C132, 3062 Defense Pentagon, Washington, DC 20301–3062. Telephone (703) 602–0311; facsimile (703) 602–0350.

List of Subjects in 48 CFR Part 252

Government procurement.

Michele P. Peterson,

Editor, Defense Acquisition Regulations System.

■ Therefore, 48 CFR Part 252 is amended as follows:

PART 252—SOLICITATION PROVISIONS AND CONTRACT CLAUSES

■ 1. The authority citation for 48 CFR Part 252 continues to read as follows:

Authority: 41 U.S.C. 421 and 48 CFR Chapter 1.

252.211–7003 [Amended]

■ 2. Section 252.211–7003 is amended as follows:
■ a. By revising the clause date to read ''(JUN 2005)';
■ b. In paragraph (c)(3)(i)(C), in the second sentence, by removing ''*http://www.acq.osd.mil/dpap/UID/guides.html*'' and adding in its place ''*http://www.acq.osd.mil/dpap/UID/guides.htm*'';
■ c. In paragraph (d) introductory text, by adding ''(1)(i) or (ii)'' after ''paragraph (c)''; and
■ d. In paragraph (e) introductory text, by removing ''*Embedded DoD serially managed subassemblies, components, and parts. The*'' and adding in its place ''For embedded DoD serially managed subassemblies, components, and parts that require unique item identification under paragraph (c)(1)(iii) of this clause, the''.

[FR Doc. 05–12095 Filed 6–20–05; 8:45 am]

BILLING CODE 5001–08–P

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

48 CFR Parts 1809, 1837, and 1852

RIN 2700–AC60

Contractor Access to Sensitive Information

AGENCY: National Aeronautics and Space Administration (NASA).

ACTION: Final rule.

SUMMARY: This final rule adopts with changes the proposed rule published in the **Federal Register** on December 5, 2003 (68 FR 67995—67998). This final rule amends the NASA Federal Acquisition Regulation (FAR) Supplement (NFS) by providing policy and procedures on how NASA will acquire services to support management activities and administrative functions when performing those services requires the contractor to have access to sensitive information submitted by other contractors. NASA's increased use of contractors to support management activities and administrative functions, coupled with implementing Agency-wide electronic information systems, requires establishing consistent procedures for protecting sensitive information from unauthorized use or disclosure.

EFFECTIVE DATE: June 21, 2005.

FOR FURTHER INFORMATION CONTACT: David Forbes, NASA Headquarters, Contract Management Division, Washington, DC 20546, (202) 358–2051, e-mail: *David.P.Forbes@nasa.gov*.

SUPPLEMENTARY INFORMATION:

A. Background

On December 5, 2003, NASA published in the **Federal Register** (68 FR 67995—67998) a proposed revision to the NFS prescribing policy, procedures, and clauses to address how NASA will acquire services to support management activities and administrative functions when performing those services requires the service provider to have access to ''confidential'' information submitted by other contractors. One of the comments that NASA received in response to this publication relates to a fundamental concept and demands attention at the outset. As published, the proposed rule used the word ''confidential'' to describe the types of information that required special attention when turned over to a service provider. NASA intended this word to describe a general class of information, largely of a business or management nature, the value of which arose mostly from the fact that it was not readily known to the public. NASA never intended this word to refer to one of the standard classifications of information for national security purposes, as in ''confidential-secret-top secret.'' Nevertheless, concerns have arisen that using the word might cause confusion with national security information. To avoid possible confusion, we have replaced the word ''confidential'' with the word ''sensitive.'' This revision should clarify that the proposed rule deals with business and management information, the value of which lies primarily in the fact that is not generally known to the public. The proposed rule does not implement or refer to the classification of information for national security purposes.

With regard to more general background information, NASA's essential procurement operations generate large amounts of ''sensitive information,'' both from offerors and contractors. Traditionally, NASA civil servants received, analyzed, and used this information to ensure that the Agency spent tax dollars in a responsible and consistent manner. The Trade Secrets Act and other statutes have for years imposed criminal liabilities on government employees who disclosed this type of information to unauthorized outside parties. Offerors and contractors have willingly provided sensitive information about their operations, costs, business practices, and other matters, knowing that NASA would not provide another contractor (''service provider'') access to this information without first ensuring that the parties had complied with FAR 9.505–4. As a condition to allowing a service provider access to another contractor's proprietary information, FAR 9.505–4 would require that the parties execute a satisfactory protection/use agreement. Central to this process were notice to the owner of the

information before any access occurred and the opportunity to develop acceptable terms and conditions governing the service provider's use of the information. From a practical standpoint, this approach could work only after the Government had selected a service provider to perform clearly defined tasks using identified information from a known source that could consent to terms and conditions governing the access.

With many more contractor personnel supporting government operations, NASA must find ways to accommodate the increasing number of situations requiring non-government personnel to safeguard contractor sensitive information. Multiple, inter-related third-party protection agreements between service providers and other contractors that submit information they claim to be ''sensitive'' will simply not work on a large scale. To establish a more efficient, realistic, modern, across-the-board solution, the NFS revisions, published for public comment in the **Federal Register** on December 5, 2003 (68 FR 67995—67998), proposed a self-executing system of procurement policy, procedures, and clauses to allow NASA activities to rely routinely on private sector service providers to support day-to-day operations throughout the Agency.

The published NFS revisions proposed two new clauses to implement this self-executing system of policies and procedures. The first clause at 1852.237–72, Access to Sensitive Information, would go into all solicitations and contracts for services to allow access to sensitive information, whenever it is needed to support NASA's management activities and administrative functions. As published, this ''Access'' clause delineated the service provider's responsibilities to limit to the purposes specified in the contract its use of any sensitive information, to safeguard the information from unauthorized outside disclosure, and to train employees and obtain their written commitments to use the information in an authorized manner, only. Because of concerns under the Paperwork Reduction Act, NASA has revised the proposed ''Access'' clause to require that the service provider obtain only a simple affirmation from each employee that he/she has received training and will comply with the lessons learned regarding the use and protection of sensitive information under the contract.

The second clause at 1852.237–73, Release of Sensitive Information, goes into all solicitations and contracts, and notifies offerors and contractors that NASA may, subject to the enumerated protections mandated by the ''Access'' clause at 1852.237–72, release their sensitive information to service providers that support NASA activities and functions. This ''Release'' clause assures offerors and contractors, by reciting the express protections incorporated into the service provider's contract through the ''Access'' clause, that their information will remain sensitive. Essentially, the ''Release'' clause announces NASA's broad intent to make necessary sensitive information available to service providers, but only in accordance with strict limitations enumerated in the companion ''Access'' clause. These enumerated limitations mandate strict, specific, and express safeguards and procedures to protect that information.

Comments on the proposed rule were received from an industry association and NASA field installations. The comments received were considered in formulation of this final rule. This final rule adopts the proposed rule with changes. The changes are made to clarify contractor roles, to emphasize the protection of sensitive information, and to provide the owners of sensitive information assurance that their data will continue to receive protection. The changes include revising the term ''receiving contractor'' to ''service provider;'' providing a sample legend to identify sensitive information; and identifying the serious consequences for unauthorized use or disclosure.

The following summarizes the comments received from NASA's publication of the proposed rule and provides responses.

1. Comment: Was it necessary for the NASA Assistant Administrator for Procurement to waive in its entirety FAR 9.505–4, Obtaining Access to Proprietary Information? Could a less drastic solution help NASA without impacting the owners of sensitive information by simply revising the NFS to relieve contracting officers of overseeing a multitude of third party protection agreements and leave the terms of protection and their enforcement to the service providers and owners, themselves? Under this approach, the contracting officer would only identify each NASA service provider to the owners of needed sensitive information and then leave these parties free to arrange for acceptable terms of protection.

Response: In a real world, competitive environment, it was necessary for NASA to waive FAR 9.505–4 in its entirety. Implicitly, FAR 9.505–4 assumes an agency has already awarded a contract to a service provider that needs access to specific information owned by another contractor. In this scenario, the protections that the owner will demand before granting access to specific sensitive information are the only significant unknowns. The assumptions behind FAR 9.505–4 are simply not valid in the early phases of a competitive procurement. Even without burdening the contracting officer to oversee third-party protection agreements, FAR 9.505–4 would require each potential service provider in a competitive procurement to know in advance of submitting a proposal, the exact information needed to perform as specified in the solicitation, what contractors own that information, and what protections those owners deemed acceptable as a condition to granting access to the information. This level of pre-proposal information would simply not be available in a competitive procurement. As a more realistic and useful alternative, the revised NFS relies not on individual third-party protection agreements, but rather prescribes standardized, reciprocal contract clauses to protect sensitive information. A ''Release'' clause goes into the information owner's contract to document consent to release and to delineate the extensive, specific protections that the service provider will implement. A reciprocal ''Access'' clause goes into the service provider's contract to place strict controls over its activities. Under the new ''Release'' clause, the owner of sensitive information expressly consents to access, as needed by NASA service providers. To gain this necessary access, however, the service provider must have expressly agreed, through the new ''Access'' clause, to comply with and implement an extensive number of binding and enumerated protections.

2. Comment: NASA has received a large quantity of ''sensitive information'' in connection with solicitations and contracts that did not contain the new ''Release'' clause. The offerors and contractors that submitted this information are not bound by the clause and have not expressly agreed that NASA service providers may have access to their sensitive information. In view of the broad waiver of FAR 9.505–4, how will NASA contracting officers avoid violating the Trade Secrets Act by giving service providers access to sensitive information that was not subject to the ''Release'' clause?

Response: This point may be valid in those situations when a service provider requests access to information that NASA has received pursuant to contracts that did not contain the

''Release'' clause. To address contracts that did not contain the clause at 1852.237–73, the NFS will provide internal guidance for NASA contracting officers and requiring activities instructing them to examine all requests from service providers for access to sensitive information. This examination should first determine whether NASA possesses responsive information. If so, the requiring activity should next assess whether access to that information is crucial to the service provider's ability to perform. If the requiring activity possesses the requested information and it is crucial to performing the needed services, then the contracting officer must try to identify and contact the owner of the information to determine whether it claims that the information is ''sensitive.'' At this point, the contracting officer should attempt to negotiate a modification to the owner's contract to incorporate the ''Release'' clause and proceed from there. Because the service provider's contract will contain extensive protections for the sensitivity of the information, NASA expects that most owners will agree to incorporate the ''Release'' clause into their existing contracts. If the owner refuses to modify its contract to include the ''Release'' clause, but persists in claiming the information is sensitive, the requiring activity should prepare a preliminary assessment for the contracting officer addressing whether the claim has a valid factual basis. This analysis should address whether NASA might have persuasive grounds to challenge the claim. If there appears to be persuasive basis for challenging the owner's claim, the contracting officer should seek advice from Center counsel before taking any further action. If, on the other hand, the claim appears to be valid, the requiring activity should re-examine the relationship of the information to the services needed. The service provider may be able to perform acceptably without the requested information. Additionally, the contracting officer may be able to facilitate reaching an agreement on acceptable terms of protection. The contracting officer and the requiring activity should examine all alternatives to obtain the needed support. But, without clear evidence that the owner of the sensitive information has consented to release, NASA will not expose its employees to the risk of violating 18 USC. 1905.

3. Comment: One comment blankly asserted that the proposed rule might violate 41 USC. 418a with respect to ''technical data.'' Although not clearly articulated, NASA assumes the comment is referring to the following language in 41 USC. 418a:

> * * * the United States may not require persons who have developed products or processes offered or to be offered for sale to the public as a condition for the procurement of such products or processes by the United States, to provide to the United States technical data relating to the design, development, or manufacture of such products or processes * * *.

Response: This prohibition deals with how Federal agencies define their procurement requirements for information. An agency may not require a company to forfeit private intellectual property rights in technical data as a condition to receiving a government contract. NASA notes simply that the proposed rule has nothing to do with defining procurement requirements for information. Rather, the proposed rule focuses on how NASA manages information that offerors and contractors have already delivered to the Government as part of submitting proposals or performing contracts. The assertion that the proposed rule might violate 41 USC. 418a appears to flow from two faulty premises. First, the proposed rule is not concerned primarily with ''technical data'' of a ''scientific or technical nature,'' but instead focuses on ''information incidental to contract administration, such as financial, administrative, cost or pricing or management information.'' The FAR expressly excludes this latter type of information from the definition of ''technical data.'' Second, the proposed rule is not concerned with how NASA defines procurement requirements for information owned by its contractors. The proposed rule simply enables service providers to obtain access to information they need to support Agency management activities and administrative functions. In most cases, the owners will have already submitted this information as a matter incidental to contract administration.

4. Comment: NASA intends to rely more and more heavily on the private sector to support essential management activities and administrative functions. Most of these activities and functions involve access to sensitive information submitted by offerors in the process of competing for awards, or by contractors as part of performance. Asking the owners of sensitive information to provide access to other contractors, some of which may be business rivals, is an inherently difficult issue and could seriously discourage competition. To promote trust, the NFS should, as a minimum, prescribe standard terms and conditions for the organizational conflicts of interest (OCI) avoidance plan and require the contracting officer to approve each offeror's proposed approach to this important document.

Response: Logically, there can be no standard approach to avoiding OCI's, which are by their nature unique to the individual contractor. The service provider must thoroughly analyze its own situation, including the services to be rendered, the information needed to perform those services, other procurements for which the service provider may intend to compete, and specific mechanisms the service provider is willing to implement to mitigate, neutralize, or eliminate foreseeable possible conflicts of interest. In addition to recognizing that each service provider's OCI's are essentially unique, any avoidance plan must flow from performance-based contracting principles to be acceptable today. As such, the buyer defines only the final outcomes to be achieved, not the methods of getting there. Consequently, the NFS will leave the details of any OCI avoidance plan to the service provider that must live by it. The contracting officer in concert with Center counsel is responsible for receiving and reviewing the plan for reasonable completeness and communicating any substantive weaknesses and omissions discovered to the service provider for necessary revisions. The contracting officer will incorporate the accepted plan into the contract as a compliance document. If the service provider fails to mitigate all potential conflicts and/or unauthorized disclosures and uses occur, the service provider must take adequate corrective actions. If the corrective actions are not adequate, the contracting officer may terminate the contract.

5. Comment: The Assistant Administrator for Procurement's broad waiver of FAR 9.505–4 could cause NASA employees to violate the Trade Secrets Act, 18 U.S.C. 1905, because not all of the information owners would have expressly consented to release through the new ''Release'' clause. Moreover, with respect to technical data, the proposed rule might also violate 41 U.S.C. 418a, which requires the FAR to prescribe regulations governing the allocation of rights in data developed through contracts using tax dollars. The Assistant Administrator's authority to waive rules relating to Organizational Conflicts of Interest does not extend the requirements of other statutes.

Response: The Trade Secrets Act prohibits government employees from releasing trade secret information to any extent not authorized by law. The Office

of Federal Procurement Policy Act authorized NASA to issue the NFS. NASA is adding the new ''Release'' clause to the NFS in accordance with the OFPP Act. Therefore, releasing information pursuant to the ''Release'' clause would be ''authorized by law'' and not violate the Trade Secrets Act. Presumably, therefore, this comment relates to sensitive information that NASA received under contracts or other agreements that did not contain the new ''Release'' clause. The NFS will contain detailed procedural guidance instructing requiring activities and contracting officers how to deal with this type of information. This procedural guidance will first instruct the contracting officer/requiring activity to contact the owner of the information to evaluate its claim to be entitled to protection and to seek agreement to incorporate the new ''Release'' clause. Alternatively, the contracting officer should try to facilitate an individualized agreement on acceptable terms of protection. If the information appears to be entitled to protection, but the owner is unwilling to accept the ''Release'' clause or to negotiate specific, tailored terms of protection, the contracting officer/requiring activity should examine on a more detailed level how much access the service provider actually needs. On closer examination, it may be possible that different, less comprehensive services could satisfy the requiring activity.

In accordance with 41 U.S.C. 418a, both the FAR and the NFS have promulgated regulations dealing with how agencies acquire and allocate rights to data developed under government contracts. The Assistant Administrator for Procurement's waiver of FAR 9.505–4 does not, however, relate to how NASA acquires and allocates rights in data. The waiver relates, instead, to information submitted in support of proposals or in the course of performing contracts. Most of this information is not ''technical data,'' which the Government procures for its own value. Rather, the revised NFS generally uses the term ''sensitive information'' to refer to financial and administrative information that is incidental to contract administration. As such, the Assistant Administrator for Procurement's waiver of FAR 9.505–4 does not affect 41 U.S.C. 418a or the requirements of any other statute or binding instruction.

6. Comment: The proposed rule does not define the term ''sensitive information'' clearly and, as a result, fails to exclude from the operation of the clauses cost or pricing data, other financial information, administrative or management information, and the like. The term ''sensitive information'' should not be broader in scope than ''data'' as defined in FAR Part 27, which specifically excludes information incidental to contract administration.

Response: NASA understands that FAR Part 27 specifically excludes information incidental to contract administration from the definition of ''data.'' In contrast, the new NFS coverage focuses primarily on information incidental to contract administration, not technical data. As the published proposed rule noted, the primary purpose of the new coverage is to allow a service provider access to information necessary to support NASA activities and functions, as civil servants did in the past.

7. Comment: The proposed rule implies that NASA need only protect data ''developed at private expense.'' The definition of ''trade secret'' does not depend on the concept of development costs. A trade secret covers a variety of forms of information that derive economic value, actual or potential, from not being generally known to the public. NASA needs to continue to protect any trade secret or it will compromise the property rights of companies, with which it currently does business. FAR 27.402 instructs agencies to avoid doing so.

Response: NASA agrees that the term ''trade secret'' extends to many types of information that derive economic value from not being generally known to the public. But, with regard to protecting contractors'' legitimate property rights, FAR 27.402 establishes the following policy: ''* * * the Government recognizes that its contractors may have a legitimate proprietary interest (*e.g.*, a property right or other valid economic interest) in data *resulting from private investment.*'' (Emphasis added.) It seems fairly clear from this language, that FAR 27.402 envisions protecting only sensitive or proprietary information that a contractor has developed at private expense. Without meeting this simple test, the FAR implicitly does not recognize as ''legitimate'' a contractor's claim for trade secret protection.

8. Comment: The revised NFS would require the holders of ''ordinary procurement'' contracts to identify ''sensitive information,'' but provides no instructions on how to do so. Moreover, NASA will continue to obtain sensitive information under contracting vehicles, such as ''Space Act Agreements,'' that are not covered by the new ''Release'' clause. What will tell these contractors how to identify ''sensitive information?''

Response: The revised NFS deals with how service providers obtain access to the information they need to support NASA operations, not with particular property rights resulting from the expenditure of tax dollars. As such, the NFS does not need to prescribe a particular legend to instruct contractors on how to identify their own sensitive information. For the contractor's convenience, however, the revised ''Release'' clause provides a sample notice identifying sensitive information. The new ''Access'' clause prescribes what service providers must do to protect the information they receive to support NASA operations. The NFS governs NASA contracts, not ''other transactions'' authorized by the Space Act. Generally, however, NASA does not acquire property and services for the expenditure of tax dollars under ''other transactions.''

9. Comment: Under the new ''Access'' clause, a service provider can allow access to sensitive information only to employees that need it to perform the specified support. Yet, the clause does not prescribe any process for determining which employees have a ''need-to-know'' sensitive information or what sanctions NASA may impose for unauthorized use.

Response: Performance-based contracting principles call for NASA to define only the final performance outcomes, not how the contractor is to achieve those objectives. The revised NFS allows the contractor to define how it will achieve the specified outcomes for NASA. Assigning work and functions among its employees is certainly within the contractor's discretion. The revised section 1837.203–70 does instruct the contracting officer to monitor the effectiveness of the contractor's system for encouraging employees to avoid unauthorized uses and disclosures. The revised clause at 1852.237–72 also describes the administrative remedies available to the contracting officer to encourage service providers to comply with their new obligations to protect sensitive information and avoid unauthorized uses or disclosures.

10. Comment: The new ''Access'' clause requires service providers to obtain express, binding written use agreements from their employees to protect sensitive information and use it only for the purposes of performing the specified services. Doing so is likely to be a tremendous administrative burden. Additionally, the service provider has no obligation to keep different companies' information segregated.

Response: As published, the new ''Access'' clause did require contractors to obtain express, binding written agreements from their employees to protect sensitive information and use it

only for performing the services specified. After considering comments on this language, NASA decided to revise the clause to require contractors to obtain written acknowledgements from their employees that they have received training in how to protect sensitive information and will adhere to the lessons learned in providing services under the contract. This simple acknowledgement does not require contractors to collect information. Certainly, a much more onerous burden would flow from a greatly expanded system of interrelated third party non-disclosure agreements among all the entities that provide sensitive information in the course of submitting competitive proposals or performing contracts for NASA. With regard to segregating different companies' information, that responsibility is implicit in the obligation to use information only to perform the specified services.

11. Comment: A potentially tremendous burden on the contracting officer, far exceeding any imposed by FAR 9.505–4, will be determining what information in NASA's possession is ''sensitive'' and who owns it. Moreover, NASA has information from companies that may no longer do business with the Government, or may no longer be in operation, at all; others have gone on to other businesses; and some may never have a contract containing the new ''Release'' clause. These situations, effectively, deprive NASA of the owner's consent to release sensitive information and expose government employees to possible violations of 18 U.S.C. 1905. If breaches and unauthorized disclosures occur, the NFS does not provide guidelines to the contracting officer on what actions are appropriate and/or effective.

Response: While some of these observations may be valid, none requires regulatory coverage beyond internal guidance for NASA operations. With regard to contracts that do not contain the ''Release'' clause, we are developing NFS internal guidance that begins by recognizing that in the course of proposing, the service provider will delve into the solicitation requirements to determine what information is needed to perform. The service provider should then request access to specifically identified information from the contracting officer/requiring activity. At that point, the requiring activity should try to determine whether NASA possesses the identified information, who owns it, and whether that owner claims to be entitled to protection. The contracting officer should then contact the owner to discuss incorporating the new ''Release'' clause. If the owner asserts the identified information is sensitive and entitled to protection, but resists incorporating the ''Release'' clause, the contracting officer should attempt to negotiate satisfactory, alternate terms of protection. The contracting officer should try to include the owner and the service provider in this process. At the same time, the contracting officer, with the assistance of Center counsel, should evaluate whether there is a valid factual basis for claiming that the information is sensitive and entitled to protection. If the owner continues to resist access, the contracting officer should, next, explore whether some reduced level of support, not requiring access to sensitive information, might be satisfactory. With regard to a service provider's unauthorized uses or disclosures, the clause at 1852.237–72 describes some of the administrative responses available to the contracting officer.

12. Comment: 1852.237–73(c) should specify whether and how the parties may challenge the sensitivity of information, including the process to follow and the owner's rights to redress.

Response: The new NFS purposely defines ''sensitive information'' to exclude ''technical data,'' as defined in the FAR. Sensitive information is incidental to contract administration and, generally, does not have independent value to its owners. Consequently, a highly structured, formalistic challenge process seems neither necessary nor desirable. Any challenge would have to show the following basic elements:

(a) Private investment developed the information or the Government generated it and it qualifies for an exception to the Freedom of Information Act.

(b) The information must not currently be in the public domain.

(c) The information may embody trade secretes or commercial or financial information.

(d) The information may be sensitive or privileged.

The NFS will provide only general guidance in this area, recognizing these are very difficult judgments. Until the contracting officer decides for sound reasons to challenge an owner's claim that information is sensitive and entitled to protection, NASA and its service provider will comply with the owner's assertions.

B. Executive Order 12866 and Regulatory Flexibility Act

This final rule does not meet the definition of ''significant'' under Executive 12866. NASA certifies that this final rule will not have a significant economic impact on a substantial number of small business entities within the meaning of the Regulatory Flexibility Act (5 U.S.C. 601, *et. seq.*), because the new, streamlined approach of having each service provider implement specific safeguards and procedures should offer the same or better protection for sensitive information belonging to small business entities than does the current system of third party agreements, envisioned by FAR 9.505–4. Moreover, this final rule should ease the burden on small business entities by not requiring them to enter multiple, interrelated third party agreements with numerous service contractors that support NASA's management activities and administrative functions.

C. Paperwork Reduction Act

The proposed NFS revisions simply amplify and clarify NASA's implementation of FAR 9.504, coverage that has existed for nearly 20 years. NASA has published these NFS revisions for public comment and received no challenges, objections, or concerns regarding the information collection requirements associated with providing services that will entail access to sensitive information. Because access to sensitive information is necessary to perform the specified services, solicitations will require all bidders and offerors to submit preliminary analyses of potential conflicts of interests. Further, each awarded contract that will entail access to sensitive information will also require the service provider to submit a comprehensive organizational conflicts of interest avoidance plan, as a deliverable report during performance.

Over the years, NASA has requested and OMB has approved various information collections necessary to evaluate bids and proposals submitted for the award of contracts, as well as for contract reports required to manage approved programs and projects. The OMB approval numbers currently in effect for these various categories of information collections are as follows:

1. OMB No. 2700–0085, bids and proposals with an estimated value more than $500,000.

2. OMB No. 2700–0089, reports required for contracts with an estimated value more than $500,000.

3. OMB No. 2700–0087, bids and proposals with an estimated value less than $500,000.

4. OMB No. 2700–0088, reports required on contracts valued at less than $500,000.

5. OMB No. 2700–0086, purchase orders for goods and services with an estimated value of $100,000 or less.

Our requests for OMB approval for these information collections have noted that NASA prepares solicitations for bids and proposals and defines requirements for contract deliverables in accordance with the OFPP Policy Act, as amended by Pub. L. 96–83, the National Aeronautics and Space Act of 1958, as amended, the Federal Acquisition Regulation (FAR), the NASA FAR Supplement, and approved mission requirements. In seeking OMB approval, NASA has described and administratively tracked these information collections in generic, functional terms, and categorized the requests based on the estimated dollar values of the purchase orders or contracts supporting the procurements in question.

As described above, these information collections cover broad functional procurement needs, at all dollar values relevant to NASA's current contracting practices. Consequently, OMB's current approvals adequately cover the proposed rule's requirements that, during the evaluation phase of each procurement, all bids and offers must contain preliminary analyses of potential conflicts of interest and that after award each new service provider must submit a comprehensive conflicts of interest avoidance plan for inclusion in the contract as a compliance document. In our view, the Paperwork Reduction Act does not require any further action in support of this final rule.

List of Subjects in 48 CFR Parts 1809, 1837, and 1852

Government Procurement.

Tom Luedtke,

Assistant Administrator for Procurement.

■ Accordingly, 48 CFR Parts 1809, 1837, and 1852 are amended as follows:

■ 1. The authority citation for 48 CFR Parts 1809, 1837, and 1852 continues to read as follows:

Authority: 42 USC. 2473(c)(1)

PART 1809—CONTRACTOR QUALIFICATIONS

■ 2. Add section 1809.505–4 to read as follows:

1809.505–4 Obtaining access to sensitive information.

(b) In accordance with FAR 9.503, the Assistant Administrator for Procurement has determined that it would not be in the Government's interests for NASA to comply strictly with FAR 9.505–4(b) when acquiring services to support management activities and administrative functions. The Assistant Administrator for Procurement has, therefore, waived the requirement that before gaining access to other companies' proprietary or sensitive (see 1837.203–70) information contractors must enter specific agreements with each of those other companies to protect their information from unauthorized use or disclosure. Accordingly, NASA will not require contractors and subcontractors and their employees in procurements that support management activities and administrative functions to enter into separate, interrelated third party agreements to protect sensitive information from unauthorized use or disclosure. As an alternative to numerous, separate third party agreements, 1837.203–70 prescribes detailed policy and procedures to protect contractors from unauthorized use or disclosure of their sensitive information. Nothing in this section waives the requirements of FAR 37.204 and 1837.204.

PART 1837—SERVICE CONTRACTING

■ 3. Add sections 1837.203–70, 1837.203–71, and 1837.203–72 to read as follows:

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.

1837.203–71 Release of contractors' sensitive information.

Pursuant to the clause at 1852.237–73, Release of Sensitive Information, offerors and contractors agree that NASA may release their sensitive information when requested by service providers in accordance with the procedures prescribed in 1837.203–70 and subject to the safeguards and protections delineated in the clause at 1852.237–72, Access to Sensitive Information. As required by the clause at 1852.237–73, or other contract clause or solicitation provision, contractors must identify information they claim to be ''sensitive'' submitted as part of a proposal or in the course of performing a contract. The contracting officer shall evaluate all contractor claims of sensitivity in deciding how NASA should respond to requests from service providers for access to information.

1837.203–72 NASA contract clauses.

(a) The contracting officer shall insert the clause at 1852.237–72, Access to Sensitive Information, in all solicitations and contracts for services that may require access to sensitive information belonging to other companies or generated by the Government.

(b) The contracting officer shall insert the clause at 1852.237–73, Release of Sensitive Information, in all solicitations, contracts, and basic ordering agreements.

PART 1852—SOLICITATION PROVISIONS AND CONTRACT CLAUSES

■ 4. Add sections 1852.237–72 and 1852.237–73 to read as follows:

1852.237–72 Access to Sensitive Information.

As prescribed in 1837.203–72(a), insert the following clause:

Access to Sensitive Information

(June 2005)

(a) As used in this clause, ''sensitive information'' refers to information that a 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, and which may embody trade secrets or commercial or financial information, and which may be sensitive or privileged.

(b) To assist NASA in accomplishing management activities and administrative functions, the Contractor shall provide the services specified elsewhere in this contract.

(c) If performing this contract entails access to sensitive information, as defined above, the Contractor agrees to—

(1) Utilize any sensitive information coming into its possession only for the purposes of performing the services specified in this contract, and not to improve its own competitive position in another procurement.

(2) Safeguard sensitive information coming into its possession from unauthorized use and disclosure.

(3) Allow access to sensitive information only to those employees that need it to perform services under this contract.

(4) Preclude access and disclosure of sensitive information to persons and entities outside of the Contractor's organization.

(5) Train employees who may require access to sensitive information about their obligations to utilize it only to perform the services specified in this contract and to safeguard it from unauthorized use and disclosure.

(6) Obtain a written affirmation from each employee that he/she has received and will comply with training on the authorized uses and mandatory protections of sensitive information needed in performing this contract.

(7) Administer a monitoring process to ensure that employees comply with all reasonable security procedures, report any breaches to the Contracting Officer, and implement any necessary corrective actions.

(d) The Contractor will comply with all procedures and obligations specified in its Organizational Conflicts of Interest Avoidance Plan, which this contract incorporates as a compliance document.

(e) The nature of the work on this contract may subject the Contractor and its employees to a variety of laws and regulations relating to ethics, conflicts of interest, corruption, and other criminal or civil matters relating to the award and administration of government contracts. Recognizing that this contract establishes a high standard of accountability and trust, the Government will carefully review the Contractor's performance in relation to the mandates and restrictions found in these laws and regulations. Unauthorized uses or disclosures of sensitive information may result in termination of this contract for default, or in debarment of the Contractor for serious misconduct affecting present responsibility as a government contractor.

(f) The Contractor shall include the substance of this clause, including this paragraph (f), suitably modified to reflect the relationship of the parties, in all subcontracts that may involve access to sensitive information

(End of clause)

1852.237–73 Release of sensitive information.

As prescribed in 1837.203–72(b), insert the following clause:

Release of Sensitive Information

(June 2005)

(a) As used in this clause, ''sensitive information'' refers to information, not currently in the public domain, that the Contractor has developed at private expense, that may embody trade secrets or commercial or financial information, and that may be sensitive or privileged.

(b) In accomplishing management activities and administrative functions, NASA relies heavily on the support of various service providers. To support NASA activities and functions, these service providers, as well as their subcontractors and their individual employees, may need access to sensitive information submitted by the Contractor under this contract. By submitting this proposal or performing this contract, the Contractor agrees that NASA may release to its service providers, their subcontractors, and their individual employees, sensitive information submitted during the course of this procurement, subject to the enumerated protections mandated by the clause at 1852.237–72, Access to Sensitive Information.

(c)(1) The Contractor shall identify any sensitive information submitted in support of this proposal or in performing this contract. For purposes of identifying sensitive information, the Contractor may, in addition to any other notice or legend otherwise required, use a notice similar to the following:

Mark the title page with the following legend:

This proposal or document includes sensitive information that NASA shall not disclose outside the Agency and its service providers that support management activities and administrative functions. To gain access to this sensitive information, a service provider's contract must contain the clause at NFS 1852.237–72, Access to Sensitive Information. Consistent with this clause, the service provider shall not duplicate, use, or disclose the information in whole or in part for any purpose other than to perform the services specified in its contract. This restriction does not limit the Government's right to use this information if it is obtained from another source without restriction. The information subject to this restriction is contained in pages [insert page numbers or other identification of pages].

Mark each page of sensitive information the Contractor wishes to restrict with the following legend:

Use or disclosure of sensitive information contained on this page is subject to the restriction on the title page of this proposal or document.

(2) The Contracting Officer shall evaluate the facts supporting any claim that particular information is ''sensitive.'' This evaluation shall consider the time and resources necessary to protect the information in accordance with the detailed safeguards mandated by the clause at 1852.237–72, Access to Sensitive Information. However, unless the Contracting Officer decides, with the advice of Center counsel, that reasonable grounds exist to challenge the Contractor's claim that particular information is sensitive,

NASA and its service providers and their employees shall comply with all of the safeguards contained in paragraph (d) of this clause.

(d) To receive access to sensitive information needed to assist NASA in accomplishing management activities and administrative functions, the service provider must be operating under a contract that contains the clause at 1852.237–72, Access to Sensitive Information. This clause obligates the service provider to do the following:

(1) Comply with all specified procedures and obligations, including the Organizational Conflicts of Interest Avoidance Plan, which the contract has incorporated as a compliance document.

(2) Utilize any sensitive information coming into its possession only for the purpose of performing the services specified in its contract.

(3) Safeguard sensitive information coming into its possession from unauthorized use and disclosure.

(4) Allow access to sensitive information only to those employees that need it to perform services under its contract.

(5) Preclude access and disclosure of sensitive information to persons and entities outside of the service provider's organization.

(6) Train employees who may require access to sensitive information about their obligations to utilize it only to perform the services specified in its contract and to safeguard it from unauthorized use and disclosure.

(7) Obtain a written affirmation from each employee that he/she has received and will comply with training on the authorized uses and mandatory protections of sensitive information needed in performing this contract.

(8) Administer a monitoring process to ensure that employees comply with all reasonable security procedures, report any breaches to the Contracting Officer, and implement any necessary corrective actions.

(e) When the service provider will have primary responsibility for operating an information technology system for NASA that contains sensitive information, the service provider's contract shall include the clause at 1852.204–76, Security Requirements for Unclassified Information Technology Resources. The Security Requirements clause requires the service provider to implement an Information Technology Security Plan to protect information processed, stored, or transmitted from unauthorized access, alteration, disclosure, or use. Service provider personnel requiring privileged access or limited privileged access to these information technology systems are subject to screening using the standard National Agency Check (NAC) forms appropriate to the level of risk for adverse impact to NASA missions. The Contracting Officer may allow the service provider to conduct its own screening, provided the service provider employs substantially equivalent screening procedures.

(f) This clause does not affect NASA's responsibilities under the Freedom of Information Act.

(g) The Contractor shall insert this clause, including this paragraph (g), suitably modified to reflect the relationship of the parties, in all subcontracts that may require the furnishing of sensitive information.

(End of clause)

[FR Doc. 05–12191 Filed 6–20–05; 8:45 am]

BILLING CODE 7510–01–P

DEPARTMENT OF TRANSPORTATION

National Highway Traffic Safety Administration

49 CFR Parts 571, 575, 577, 582

[Docket No. NHTSA–2005–21564]

Vehicle Safety Hotline; Technical Amendment

AGENCY: National Highway Traffic Safety Administration (NHTSA), Department of Transportation.

ACTION: Final rule; technical amendment.

SUMMARY: This document contains technical amendments to Part 571, *Federal motor vehicle safety standards;* Part 575, *Consumer information;* Part 577, *Defect and noncompliance notification;* and Part 582, *Insurance cost information regulation.* Specifically, we are updating the telephone number that should be used to reach NHTSA's Vehicle Safety Hotline, and adding our web address. This amendment updates the pertinent contact information without making any substantive changes to our regulations.

DATES: The technical amendments to parts 571, 575, and 582 are effective June 21, 2006. The technical amendment to Part 577 is effective July 21, 2005. Voluntary compliance is permitted before that time.

FOR FURTHER INFORMATION CONTACT: Mr. George Feygin, Office of Chief Counsel (Telephone: 202–366–2992) (Fax: 202–366–3820); NHTSA, 400 Seventh Street, SW., Washington, DC 20590.

SUPPLEMENTARY INFORMATION: In several regulations, NHTSA specifies that vehicle manufacturers, child seat manufacturers, or automobile dealers must provide the telephone number for our Vehicle Safety Hotline so that consumers concerned about safety recalls or potential defects could contact this agency. That telephone number has changed. This document amends the relevant sections of the CFR to correct the telephone number and to add our web address so that consumers can access the safety recall and defect information online. We are also changing the text in the Part 582 information form to reflect our current New Car Assessment Program efforts.

This technical amendment will not impose or relax any substantive requirements or burdens on manufacturers. Except for Part 577, we are providing a lead-time of one year in order to afford affected parties time to update the relevant contact information where necessary. Therefore, NHTSA finds for good cause that any notice and opportunity for comment on these correcting amendments are not necessary.

In consideration of the foregoing, this document amends the CFR by updating the contact information for the Vehicle Safety Hotline.

List of Subjects in 49 CFR Parts 571, 575, 577, 582

Consumer protection; Insurance; Motor vehicles; Motor vehicle safety; Reporting and recordkeeping requirements; Tires.

■ 49 CFR Parts 571, 575, 577, 582 are amended by making the following technical amendments:

PART 571—FEDERAL MOTOR VEHICLE SAFETY STANDARDS

■ 1. The authority citation continues to read as follows:

Authority: 49 U.S.C. 322, 2011, 30115, 30166 and 30177; delegation of authority at 49 CFR 1.50.

■ 2. Section 571.213 is amended by revising sections S5.5.2(m), S5.5.5(k), S5.6.1.7, and S5.6.2.2 to read as follows:

§ 571.213 Standard No. 213; Child restraint systems.

* * * * *

S5.5.2 * * *

(m) The following statement, inserting an address and telephone number: ''Child restraints could be recalled for safety reasons. You must register this restraint to be reached in a recall. Send your name, address and the restraint's model number and manufacturing date to (insert address) or call (insert telephone number). For recall information, call the U.S. Government's Vehicle Safety Hotline at 1–888–327–4236 (TTY: 1–800–424–9153), or go to *http://www.NHTSA.gov.*''

* * * * *

(k) The following statement, inserting an address and telephone number: ''Child restraints could be recalled for safety reasons. You must register this restraint to be reached in a recall. Send your name, address and the restraint's model number and manufacturing date to (insert address) or call (insert telephone number). For recall information, call the U.S. Government's Vehicle Safety Hotline at 1–888–327–