and the timing of that auction did not prevent the participation of small businesses in the 800 MHz SMR auction, in which 52 of the 62 qualified bidders were eligible for small or very small business credits.

5. Second, the Commission rejects the claim that the Bureau's authority to set the level of upfront payments constitutes an illegal delegation of authority. Section 0.131 of the Commission's rules explicitly states that the Bureau has delegated authority to develop, recommend and administer policies, programs and rules concerning auctions of spectrum for wireless telecommunications. In the Amendment of Part 1 of the Commission's Rules to Facilitate Future Development of SMR Systems in the 800 MHz Frequency Band, *Order and Memorandum Opinion & Order (Part 1 Order)*, 62 FR 13540 (March 21, 1997), rulemaking, the Commission clarified that pursuant to § 0.131 of its rules, the Chief of the Wireless Telecommunications Bureau has delegated authority to implement all of the Commission's rules pertaining to auctions procedures. This includes the authority to choose competitive bidding designs and methodologies; conduct auctions; administer application, payment, licenses grant and denial procedures; and determine upfront and down payment amounts as well as minimum opening bids. These actions do not fall under the prohibited activities set forth in § 0.331 of the Commission's rules, which include acting upon complaints, petitions, requests, applications for review and notices of proposed rulemaking. The Commission concludes that the Bureau's actions are valid, as they affect procedural rather than substantive issues, and are, therefore, in compliance with our rules. Furthermore, the Bureau's actions were in compliance with the APA. Pursuant to 5 U.S.C. 553(b), an agency may modify procedural rules without notice and comment. Because the rule modifications were procedural in nature and did not affect the substantive rights of interested parties, the Bureau's actions fall within that exception.

6. Third, the Commission dismisses as repetitions the request that it reconsider its decisions to allocate licenses in the upper 200 channels of the 800 MHz SMR spectrum in contiguous blocks, eliminate the finder's preference program, and use competitive bidding as the licensing mechanism for the upper 200 channels in the 800 MHz band. The Commission disagrees with petitioner's contention that these decisions were unsupported by evidence and therefore, arbitrary and capricious. These conclusions were set forth first in the Amendment of Part 1 of the Commission's Rules to Facilitate Future Development of SMR Systems in the 800 MHz Frequency Band, *First Report and Order, Eighth Report and Order and Second Further Notice of Proposed Rulemaking (First R&O)*, 61 FR 6212 (February 16, 1996), and reaffirmed in the *First MO&O*. In each case, the Commission set forth reasoned explanations for its decision. It is not in the public interest to revisit these issues.

7. Finally, the Commission finds it unnecessary to address the request for clarification of the Commission's decision to require incumbents seeking geographic licenses to show that their facilities are constructed and operational. In the *First R&O*, the Commission stated that such licensees are required to make a one-time filing of specific information for each of their external base station sites to assist the staff in updating the Commission database after the close of the auction for the upper 200 channels of the 800 MHz SMR spectrum. Under that decision, the Commission also requires evidence that such facilities are constructed and placed in operation and that, by operation of its rules, no other licensees would be able to use these channels within a geographic area.

8. It is ordered that the Petitions are denied.

List of Subjects in 47 CFR Part 90

Radio.

Federal Communications Commission.

Magalie Roman Salas,

Secretary.

[FR Doc. 00–17848 Filed 7–13–00; 8:45 am]

BILLING CODE 6712–01–P

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

48 CFR Parts 1804 and 1852

Security Requirements for Unclassified Information Technology Resources

AGENCY: National Aeronautics and Space Administration.

ACTION: Final Rule.

SUMMARY: This final rule amends the NASA FAR Supplement (NFS) to: include a requirement for contractors and subcontractors working with NASA unclassified Information Technology Systems to take certain Information Technology (IT) security related actions; document those actions; and submit related reports to NASA.

EFFECTIVE DATE: July 14, 2000.

FOR FURTHER INFORMATION CONTACT: Karl Beisel, NASA Headquarters (Code HC), Washington, DC, (202) 358–0416, email: *Karl.Beisel@hq.nasa.gov.*

SUPPLEMENTARY INFORMATION:

A. Background

A proposed rule was published in the **Federal Register** on January 5, 2000 (65 FR 429–431). Comments were received from two respondents, an industry association and the NASA Office of Inspector General (OIG). All comments were considered in the development of this final rule. This final rule includes changes for clarification of meaning, consistency of wording (and phrasing), and to eliminate informational redundancies within the clause as it references information in other related documents.

This final rule requires NASA contractors and subcontractors to comply with the security requirements outlined in NASA Policy Directive (NPD) 2810.1, Security of Information Technology, and NASA Procedures and Guidelines (NPG) 2810.1, Security of Information Technology, and additional safeguarding requirements delineated in the contract clause. Currently, NASA contractors have no definitive contractual requirement to follow NASA directed policy in safeguarding unclassified NASA data held via information technology (computer systems). This final rule establishes these requirements in a contract clause. These policies apply to all IT systems and networks under NASA's purview operated by or on behalf of the Federal Government, regardless of location.

B. Regulatory Flexibility Act

NASA certifies that this final rule will not have a significant economic impact on a substantial number of small entities within the meaning of the Regulatory Flexibility Act, 5 U.S.C. 601 *et seq.* The changes merely formalize standard procedures in using Government computer systems and databases. Small entities will not need to significantly revise internal procedures to satisfy the NFS changes.

C. Paperwork Reduction Act

An Office of Management and Budget (OMB) approval for data collection has been approved under OMB Control No. 2700–0098.

List of Subjects in 48 CFR Parts 1804 and 1852.

Government procurement.

Tom Luedtke,

Associate Administrator for Procurement.

Accordingly, 48 CFR Parts 1804 and 1852 are amended as follows:

1. The authority citation of 48 CFR Parts 1804 and 1852 continues to read as follows:

Authority: 42 U.S.C. 2473(c)(1).

PART 1804—ADMINISTRATIVE MATTERS

2. Revise the title of section 1804.470 to read as follows:

1804.470 Security requirements for unclassified information technology resources.

3. Revise sections 1804.470–2, 1804.470–3, and 1804.470–4 to read as follows:

1804.470–2 Policy.

(a) NASA policies and procedures on security for automated information technology are prescribed in NPD 2810.1, Security of Information Technology, and in NPG 2810.1, Security of Information Technology. Security requirements for safeguarding sensitive information contained in unclassified Federal computer systems are required in the following:

(1) All contracts for information technology resources or services. This includes, but is not limited to information technology hardware, software, and the management, operation, maintenance, programming, and system administration of information technology resources, to include computer systems, networks, and telecommunications systems.

(2) Contracts under which contractor personnel must have physical or electronic access to NASA's sensitive information contained in unclassified systems or information technology services that directly support the mission of the agency.

(b) The contractor must not use or redistribute any NASA information processed, stored, or transmitted by the contractor except as specified in the contract.

1804.470–3 Security plan for unclassified Federal Information Technology systems.

(a) The contracting officer, with the concurrence of the requiring activity, the center Chief Information Officer (CIO), and the center Information Technology (IT) Security Manager, may require the contractor to submit for post-award Government approval, a detailed Security Plan for Unclassified Federal Information Technology Systems. The plan must be required as a contract data deliverable that must be subsequently incorporated into the contract as a compliance document after Government approval. The plan must demonstrate a thorough understanding of NPG 2810.1 and NPD 2810.1 and must include, as a minimum, the security measures and program safeguards planned to ensure that the information technology resources acquired and used by contractor and subcontractor personnel—

(1) Are protected from unauthorized access, alteration, disclosure, or misuse of information processed, stored, or transmitted;

(2) Can maintain the continuity of automated information support for NASA missions, programs, and functions;

(3) Incorporate management, general, and application controls sufficient to provide cost-effective assurance of the systems' integrity and accuracy;

(4) Have appropriate technical, personnel, administrative, environmental, and access safeguards;

(5) Document and follow a virus protection program for all IT resources under its control; and

(6) Document and follow a network intrusion detection and prevention program for all IT resources under its control.

(b) The contractor must be required to develop and maintain IT System Security Plans, in accordance with NPG 2810.1, for systems for which the contractor has primary operational responsibility on behalf of NASA.

1804.470–4 Contract clauses.

The contracting officer must insert the clause at 1852.204–76, Security Requirements for Unclassified Information Technology Resources, in solicitations and contracts involving unclassified information technology resources.

PART 1852—SOLICITATION PROVISIONS AND CONTRACT CLAUSES

3. Revise section 1852.204–76 to read as follows:

1852.204–76 Security Requirements for Unclassified Information Technology Resources.

As prescribed in 1804.470–4, insert the following clause:

Security Requirements for Unclassified Information Technology Resources July, 2000

(a) The Contractor shall comply with the security requirements outlined in NASA Policy Directive (NPD) 2810.1, Security of Information Technology, and NASA Procedures and Guidelines (NPG) 2810.1, Security of Information Technology. These policies apply to all IT systems and networks under NASA's purview operated by or on behalf of the Federal Government, regardless of location.

(b)(1) The Contractor shall ensure compliance by its employees with Federal directives and guidelines that deal with IT Security including, but not limited to, OMB Circular A–130, Management of Federal Information Resources, OMB Circular A–130 Appendix III, Security of Federal Automated Information Resources, the Computer Security Act of 1987 (40 U.S.C. 1441 *et seq.*), and all applicable Federal Information Processing Standards (FIPS).

(2) All Federally owned information is considered sensitive to some degree and must be appropriately protected by the Contractor as specified in applicable IT Security Plans. Types of sensitive information that may be found on NASA systems that the Contractor may have access to include, but are not limited to—

(i) Privacy Act information (5 U.S.C. 552a *et seq.*);

(ii) Export Controlled Data, (e.g. Resources protected by the International Traffic in Arms Regulations (22 CFR Parts 120–130)).

(3) The Contractor shall ensure that all systems connected to a NASA network or operated by the Contractor for NASA conform with NASA and Center security policies and procedures.

(c)(1) The Contractor's screening of Contractor personnel will be conducted in accordance with NPG 2810.1, Section 4.5 for personnel requiring unescorted or unsupervised physical or electronic access to NASA systems, programs, and data.

(2) The Contractor shall ensure that all such employees have at least a National Agency Check investigation. The Contractor shall submit a personnel security questionnaire (NASA Form 531), Name Check Request for National Agency Check (NAC) investigation, and Standard Form 85P, Questionnaire for Public Trust Positions (for specified sensitive positions), and a Fingerprint Card (FD–258 with NASA overprint in Origin Block) to the Center Chief of Security for each Contractor employee requiring screening. The required forms may be obtained from the Center Chief of Security. In the event that the NAC is not satisfactory, access shall not be granted. At the option of the Government, background screenings may not be required for employees with recent or current Federal Government investigative clearances.

(3) The Contractor shall have an employee checkout process that ensures—

(i) Return of badges, keys, electronic access devices and NASA equipment;

(ii) Notification to NASA of planned employee terminations at least three days in advance of the employee's departure. In the case of termination for cause, NASA shall be notified immediately. All NASA accounts and/or network access granted terminated employees shall be disabled immediately upon the employee's separation from the Contractor; and

(iii) That the terminated employee has no continuing access to

systems under the operation of the Contractor for NASA. Any access must be disabled the day the employee separates from the Contractor.

(4) Granting a non-permanent resident alien (foreign national) access to NASA IT resources requires special authorization. The Contractor shall obtain authorization from the Center Chief of Security prior to granting a non-permanent resident alien access to NASA IT systems and networks.

(d)(1) The Contractor shall ensure that its employees with access to NASA information resources receive annual IT security awareness and training in NASA IT Security policies, procedures, computer ethics, and best practices.

(2) The Contractor shall employ an effective method for communicating to all its employees and assessing that they understand any Information Technology Security policies and guidance provided by the Center Information Technology Security Manager (CITSM) and/or Center CIO Representative as part of the new employee briefing process. The Contractor shall ensure that all employees represent that they have read and understand any new Information Technology Security policy and guidance provided by the CITSM and Center CIO Representative over the duration of the contract.

(3) The Contractor shall ensure that its employees performing duties as system and network administrators in addition to performing routine maintenance possess specific IT security skills. These skills include the following:

(i) Utilizing software security tools.

(ii) Analyzing logging and audit data.

(iii) Responding and reporting to computer or network incidents as per NPG 2810.1.

(iv) Preserving electronic evidence as per NPG 2810.1.

(v) Recovering to a safe state of operation.

(4) The Contractor shall provide training to employees to whom they plan to assign system administrator roles. That training shall provide the employees with a full level of proficiency to meet all NASA system administrators' functional requirements. The Contractor shall have methods or processes to document that employees have mastered the training material, or have the required knowledge and skills. This applies to all system administrator requirements.

(e) The Contractor shall promptly report to the Center IT Security Manager any suspected computer or network security incidents occurring on any system operated by the Contractor for NASA or connected to a NASA network. If it is validated that there is an incident, the Contractor shall provide access to the affected system(s) and system records to NASA and any NASA designated third party so that a detailed investigation can be conducted.

(f) The Contractor shall develop procedures and implementation plans that ensure that IT resources leaving the control of an assigned user (such as being reassigned, repaired, replaced, or excessed) have all NASA data and sensitive application software permanently removed by a NASA-approved technique. NASA-owned applications acquired via a ''site license'' or ''server license'' shall be removed prior to the resources leaving NASA's use. Damaged IT storage media for which data recovery is not possible shall be degaussed or destroyed. If the assigned task is to be assumed by another duly authorized person, at the Government's option, the IT resources may remain intact for assignment and use of the new user.

(g) The Contractor shall afford NASA, including the Office of Inspector General, access to the Contractor's and subcontractor's facilities, installations, operations, documentation, databases and personnel. Access shall be provided to the extent required to carry out a program of IT inspection, investigation and audit to safeguard against threats and hazards to the integrity, availability and confidentiality of NASA data, and to preserve evidence of computer crime.

(h)(1) The Contractor shall document all vulnerability testing and risk assessments conducted in accordance with NPG 2810.1 and any other IT security requirements specified in the contract or as directed by the Contracting Officer.

(2) The results of these tests shall be provided to the Center IT Security Manager. Any Contractor system(s) connected to a NASA network or operated by the Contractor for NASA may be subject to vulnerability assessment or penetration testing as part of the Center's IT security compliance assessment and the Contractor shall be required to assist in the completion of these activities.

(3) A decision to accept any residual risk shall be the responsibility of NASA. The Contractor shall notify the NASA system owner and the NASA data owner within 5 working days if new or unanticipated threats or hazards are discovered by the Contractor, made known to the Contractor, or if existing safeguards fail to function effectively. The Contractor shall make appropriate risk reduction recommendations to the NASA system owner and/or the NASA data owner and document the risk or modifications in the IT Security Plan.

(i) The Contractor shall develop a procedure to accomplish the recording and tracking of IT System Security Plans, including updates, and IT system penetration and vulnerability tests for all NASA systems under its control or for systems outsourced to them to be managed on behalf of NASA. The Contractor must report the results of these actions directly to the Center IT Security Manager.

(j) When directed by the Contracting Officer, the Contractor shall submit for NASA approval a post-award security implementation plan outlining how the Contractor intends to meet the requirements of NPG 2810.1. The plan shall subsequently be incorporated into the contract as a compliance document after receiving Government approval. The plan shall demonstrate thorough understanding of NPG 2810.1 and shall include as a minimum, the security measures and program safeguards to ensure that IT resources acquired and used by Contractor and subcontractor personnel—

(1) Are protected from unauthorized access, alteration, disclosure, or misuse of information processed, stored, or transmitted;

(2) Can maintain the continuity of automated information support for NASA missions, programs, and functions;

(3) Incorporate management, general, and application controls sufficient to provide cost-effective assurance of the systems' integrity and accuracy;

(4) Have appropriate technical, personnel, administrative, environmental, and access safeguards;

(5) Document and follow a virus protection program for all IT resources under its control; and

(6) Document and follow a network intrusion prevention program for all IT resources under its control.

(k) Prior to selecting any IT security solution, the Contractor shall consult with their Center IT Security Manager to ensure interoperability and compatibility with other systems with which there is a data or system interface requirement.

(l) The Contractor shall comply with all Federal and NASA encryption requirements for NASA flight programs (*e.g.,* secure flight termination systems, encryption for satellite uplinks, encryption for flight and satellite command and control for both up and down link) and involve the Center Communications Security (COMSEC) Manager when selecting encryption solutions.

(m) The Contractor shall incorporate this clause in all subcontracts where the requirements identified in this clause are applicable to the performance of the subcontract.

(End of clause)

[FR Doc. 00–17881 Filed 7–13–00; 8:45 am]

BILLING CODE 7510–01–U