

(End of clause)

[61 FR 40548, Aug. 5, 1996]

**1852.204-76 Security Requirements for
Unclassified Information Tech-
nology Resources.**

As prescribed in 1804.470-4, insert a clause substantially as follows:

SECURITY REQUIREMENTS FOR UNCLASSIFIED
INFORMATION TECHNOLOGY RESOURCES,
(JUL 2002)

(a) The Contractor shall be responsible for Information Technology security for all systems connected to a NASA network or operated by the Contractor for NASA, regardless of location. This clause is applicable to all or any part of the contract that includes information technology resources or services in which the Contractor must have physical or electronic access to NASA's sensitive information contained in unclassified systems that directly support the mission of the Agency. This includes information technology, hardware, software, and the management, operation, maintenance, programming, and system administration of computer systems, networks, and telecommunications systems. Examples of tasks that require security provisions include:

- (1) Computer control of spacecraft, satellites, or aircraft or their payloads;
- (2) Acquisition, transmission or analysis of data owned by NASA with significant replacement cost should the contractor's copy be corrupted; and
- (3) Access to NASA networks or computers at a level beyond that granted the general public, *e.g.* bypassing a firewall.

(b) The Contractor shall provide, implement, and maintain an IT Security Plan. This plan shall describe the processes and procedures that will be followed to ensure appropriate security of IT resources that are developed, processed, or used under this contract. The plan shall describe those parts of the contract to which this clause applies. The Contractor's IT Security Plan shall be compliant with Federal laws that include, but are not limited to, the Computer Security Act of 1987 (40 U.S.C. 1441 *et seq.*) and the Government Information Security Reform Act of 2000. The plan shall meet IT security requirements in accordance with Federal and NASA policies and procedures that include, but are not limited to:

- (1) OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources;
- (2) NASA Procedures and Guidelines (NPG) 2810.1, Security of Information Technology; and
- (3) Chapter 3 of NPG 1620.1, NASA Security Procedures and Guidelines.

(c) Within ___ days after contract award, the contractor shall submit for NASA approval an IT Security Plan. This plan must be consistent with and further detail the approach contained in the offeror's proposal or sealed bid that resulted in the award of this contract and in compliance with the requirements stated in this clause. The plan, as approved by the Contracting Officer, shall be incorporated into the contract as a compliance document.

(d)(1) Contractor personnel requiring privileged access or limited privileged access to systems operated by the Contractor for NASA or interconnected to a NASA network shall be screened at an appropriate level in accordance with NPG 2810.1, Section 4.5; NPG 1620.1, Chapter 3; and paragraph (d)(2) of this clause. Those Contractor personnel with non-privileged access do not require personnel screening. NASA shall provide screening using standard personnel screening National Agency Check (NAC) forms listed in paragraph (d)(3) of this clause, unless contractor screening in accordance with paragraph (d)(4) is approved. The Contractor shall submit the required forms to the NASA Center Chief of Security (CCS) within fourteen (14) days after contract award or assignment of an individual to a position requiring screening. The forms may be obtained from the CCS. At the option of the government, interim access may be granted pending completion of the NAC.

(2) Guidance for selecting the appropriate level of screening is based on the risk of adverse impact to NASA missions. NASA defines three levels of risk for which screening is required (IT-1 has the highest level of risk):

(i) IT-1—Individuals having privileged access or limited privileged access to systems whose misuse can cause very serious adverse impact to NASA missions. These systems include, for example, those that can transmit commands directly modifying the behavior of spacecraft, satellites or aircraft.

(ii) IT-2—Individuals having privileged access or limited privileged access to systems whose misuse can cause serious adverse impact to NASA missions. These systems include, for example, those that can transmit commands directly modifying the behavior of payloads on spacecraft, satellites or aircraft; and those that contain the primary copy of "level 1" data whose cost to replace exceeds one million dollars.

(iii) IT-3—Individuals having privileged access or limited privileged access to systems whose misuse can cause significant adverse impact to NASA missions. These systems include, for example, those that interconnect with a NASA network in a way that exceeds access by the general public, such as bypassing firewalls; and systems operated by the contractor for NASA whose function or data has substantial cost to replace, even if these

systems are not interconnected with a NASA network.

(3) Screening for individuals shall employ forms appropriate for the level of risk as follows:

(i) IT-1: Fingerprint Card (FC) 258 and Standard Form (SF) 85P, Questionnaire for Public Trust Positions;

(ii) IT-2: FC 258 and SF 85, Questionnaire for Non-Sensitive Positions; and

(iii) IT-3: NASA Form 531, Name Check, and FC 258.

(4) The Contracting Officer may allow the Contractor to conduct its own screening of individuals requiring privileged access or limited privileged access provided the Contractor can demonstrate that the procedures used by the Contractor are equivalent to NASA's personnel screening procedures. As used here, equivalent includes a check for criminal history, as would be conducted by NASA, and completion of a questionnaire covering the same information as would be required by NASA.

(5) Screening of contractor personnel may be waived by the Contracting Officer for those individuals who have proof of—

(1) Current or recent national security clearances (within last three years);

(ii) Screening conducted by NASA within last three years; or

(iii) Screening conducted by the Contractor, within last three years, that is equivalent to the NASA personnel screening procedures as approved by the Contracting Officer under paragraph (d)(4) of this clause.

(e) The Contractor shall ensure that its employees, in performance of the contract, receive annual IT security training in NASA IT Security policies, procedures, computer ethics, and best practices in accordance with NPG 2810.1, Section 4.3 requirements. The contractor may use web-based training available from NASA to meet this requirement.

(f) The Contractor shall afford NASA, including the Office of Inspector General, access to the Contractor's and subcontractors' facilities, installations, operations, documentation, databases and personnel used in performance of the contract. 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 or to the function of computer systems operated on behalf of NASA, and to preserve evidence of computer crime.

(g) The Contractor shall incorporate the substance of this clause in all subcontracts that meet the conditions in paragraph (a) of this clause.

(End of clause)

[66 FR 36491, July 12, 2001, as amended at 67 FR 48815, July 26, 2002]

1852.208-81 Restrictions on Printing and Duplicating.

As prescribed in 1808.870, insert the following clause:

RESTRICTIONS ON PRINTING AND DUPLICATING OCTOBER 2001

(a) The Contractor may duplicate or copy any documentation required by this contract in accordance with the provisions of the Government Printing and Binding Regulations, No. 26, S. Pub 101-9, U.S. Government Printing Office, Washington, DC, 20402, published by the Joint Committee on Printing, U.S. Congress.

(b) The Contractor shall not perform, or procure from any commercial source, any printing in connection with the performance of work under this contract. The term "printing" includes the processes of composition, platemaking, presswork, duplicating, silk screen processes, binding, microform, and the end items of such processes and equipment.

(c) The Contractor is authorized to duplicate or copy production units provided the requirement does not exceed 5,000 production units of any one page or 25,000 units in the aggregate of multiple pages. Such pages may not exceed a maximum image size of 10-3/4 by 14-1/4 inches. A "production unit" is one sheet, size 8-1/2x11 inches (215x280 mm), one side only, and one color ink.

(d) This clause does not preclude writing, editing, preparation of manuscript copy, or preparation of related illustrative material as a part of this contract, or administrative duplicating/copying (for example, necessary forms and instructional materials used by the Contractor to respond to the terms of the contract).

(e) Costs associated with printing, duplicating, or copying in excess of the limits in paragraph (c) of this clause are unallowable without prior written approval of the Contracting Officer. If the Contractor has reason to believe that any activity required in fulfillment of the contract will necessitate any printing or substantial duplicating or copying, it immediately shall provide written notice to the Contracting Officer and request approval prior to proceeding with the activity. Requests will be processed by the Contracting Officer in accordance with the provisions of the Government Printing and Binding Regulations, NFS 1808.802, and NPG 1490.5, NASA Procedures and Guidelines for Printing, Duplicating, and Copying Management.

(f) The Contractor shall include in each subcontract which may involve a requirement for any printing, duplicating, and copying in excess of the limits specified in paragraph (c) of this clause, a provision substantially the same as this clause, including this paragraph (f).