compromise or denial of information technology services; damage or loss greater than $250,000 to the Government; or theft.

(b) In the event of a major breach of safety or security, the Recipient shall report the breach to the Agreement Officer. If directed by the Agreement Officer, the Recipient shall conduct its own investigation and report the results to the Government. The Recipient shall cooperate with the Government investigation, if conducted.

[End of provision]

§ 1274.937 Security requirements for unclassified information technology resources.

SECURITY REQUIREMENTS FOR UNCLASSIFIED INFORMATION TECHNOLOGY RESOURCES

July 2002

(a) The Recipient shall be responsible for Information Technology security for all systems connected to a NASA network or operated by the Recipient for NASA, regardless of location. This provision is applicable to all or any part of the cooperative agreement that includes information technology resources or services in which the Recipient 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 Recipient'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 Recipient 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 cooperative agreement. The plan shall describe those parts of the cooperative agreement to which this provision applies. The Recipient'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 cooperative agreement award, the Recipient shall submit for NASA approval an IT Security Plan. This plan must be consistent with and further detail the approach contained in the Recipient's proposal that resulted in the award of this cooperative agreement and in compliance with the requirements stated in this provision. The plan, as approved by the Agreement Officer, shall be incorporated into the cooperative agreement as a compliance document.

(d)(1) Recipient personnel requiring privileged access or limited privileged access to systems operated by the Recipient 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 provision. Those Recipient 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 provision, unless Recipient screening in accordance with paragraph (d)(4) is approved. The Recipient shall submit the required forms to the NASA Center Chief of Security (CCS) within fourteen (14) days after cooperative agreement 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 Recipient 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 Agreement Officer may allow the Recipient to conduct its own screening of individuals requiring privileged access or limited privileged access provided the Recipient can demonstrate that the procedures used by the Recipient 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 Recipient personnel may be waived by the Agreement Officer for those individuals who have proof of—

(i) 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 Recipient, within last three years, that is equivalent to the NASA personnel screening procedures as approved by the Agreement Officer under paragraph (d)(4) of this provision.

(e) The Recipient shall ensure that its employees, in performance of the cooperative agreement, 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 Recipient may use web-based training available from NASA to meet this requirement.

(f) The Recipient shall afford NASA, including the Office of Inspector General, access to the Recipient's, subcontractors' or subawardees' facilities, installations, operations, documentation, databases and personnel used in performance of the cooperative agreement. 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 Recipient shall incorporate the substance of this clause in all subcontracts or subagreements that meet the conditions in paragraph (a) of this provision.

[End of provision]

§ 1274.938 Modifications.

MODIFICATIONS

July 2002

During the term of this agreement and in the interest of achieving program objectives, the parties may agree to changes that affect the responsibility statements, milestones, or other provisions of this agreement. Any changes to this agreement will be accomplished by a written bilateral modification.

[End of provision]

§ 1274.939 Application of Federal, State, and Local laws and regulations.

APPLICATION OF FEDERAL, STATE, AND LOCAL LAWS AND REGULATIONS

July 2002

(a) *Federal Laws and Regulations.* This Cooperative Agreement shall be governed by the Federal Laws, regulations, policies, and related administrative practices applicable to this Cooperative Agreement on the date the Agreement is executed. The Recipient understands that such Federal laws, regulations, policies, and related administrative practices may be modified from time to time. The Recipient agrees to consider modifying this Agreement to be governed by those later modified Federal laws, regulations, policies, and related administrative practices that directly affect performance of the Project.

(b) *State or Territorial Law and Local Law.* Except to the extent that a Federal statute or regulation preempts State or territorial law, nothing in the Cooperative Agreement shall require the Recipient to observe or enforce compliance with any provision thereof, perform any other act, or do any other thing in contravention of any applicable State or territorial law; however, if any of the provisions of the Cooperative Agreement violate any applicable State or territorial law, or if compliance with the provisions of the Agreement would require the Recipient to violate any applicable State or territorial law, the Recipient agrees to notify the Government (NASA) immediately in writing in order that the Government and the Recipient may