§ 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. 141 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:

2. NASA Procedures and Guidelines (NPG) 2810.1, Security of Information Technology; and

(c) Within 14 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 cooperation 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.

(d)(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):

1. 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.
2. 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
§ 1274.938 Application of Federal, State, and Local laws and regulations.

(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, the Recipient agrees to notify the Government (NASA) immediately in writing in order that the Government and the Recipient may