| Report | Frequency | Reference |
|---|---|---|
| Summary of Research | 90 days after completion of agreement | 1274.921 Publications and Reports: Non-Proprietary Research Results (Paragraph (d)(2)) |
| NASA Form 1018 Property in the Custody of Contractors. | Annually by October 15 | 1274.923 Equipment and Other Property (Paragraph (f)) |
| NASA Form 1018 Property in the Custody of Contractors. | 60 days after expiration date of agreement. | 1274.923 Equipment and Other Property (Paragraph (f)) |

[67 FR 45790, July 10, 2002, as amended at 69 FR 41936, July 13, 2004]

### § 1274.934 Safety.

SAFETY

July 2002

NASA's safety priority is to protect: (1) The public, (2) astronauts and pilots, (3) the NASA workforce (including contractor employees working on NASA contracts), and (4) high-value equipment and property.

(a) The Recipient shall act responsibly in matters of safety and shall take all reasonable safety measures in performing under this cooperative agreement. The recipient shall comply with all applicable federal, state, and local laws relating to safety. The Recipient shall maintain a record of, and will notify the NASA Agreement Officer immediately (within one workday) of any accident involving death, disabling injury or substantial loss of property. The Recipient will immediately (within one workday) advise NASA of hazards that come to its attention as a result of the work performed.

(b) Where the work under this cooperative agreement involves flight hardware, the hazardous aspects, if any, of such hardware will be identified, in writing, by the Recipient. Compliance with this provision by subcontractors shall be the responsibility of the Recipient.

[End of provision]

### § 1274.935 Security classification requirements.

SECURITY CLASSIFICATION REQUIREMENTS

July 2002

Performance under this Cooperative Agreement will involve access to and/or generation of classified information, work in a secure area, or both, up to the level of [*insert the applicable security clearance level*]. Federal Acquisition Regulation clause 52.204–2 shall apply to this Agreement and DD Form 254, Contract Security Classification Specification Attachment _____ [*Insert the attachment number of the DD Form 254.*]

[End of provision]

### § 1274.936 Breach of safety or security.

BREACH OF SAFETY OR SECURITY

July 2002

Safety is the freedom from those conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment. Safety is essential to NASA and is a material part of this contract. NASA's safety priority is to protect: The public; astronauts and pilots; the NASA workforce (including contractor employees working on NASA contracts); and high-value equipment and property. A major breach of safety by the Recipient entitles the Government to remedies (pending corrective measures by the Recipient) which includes, suspension or termination of the Cooperative Agreement, require removal or change of Recipient's personnel from performing under the Agreement. A major breach of safety must be related directly to the work on the Agreement. A major breach of safety is an act or omission of the Recipient that consists of an accident, incident, or exposure resulting in a fatality or mission failure; or in damage to equipment or property equal to or greater than $1 million; or in any ''willful'' or ''repeat'' violation cited by the Occupational Safety and Health Administration (OSHA) or by a state agency operating under an OSHA approved plan.

(a) Security is the condition of safeguarding against espionage, sabotage, crime (including computer crime), or attack. A major breach of security by the Recipient entitles the Government to remedies (pending corrective measures by the Recipient) which includes, suspension or termination of the Cooperative Agreement, require removal or change of Recipient's personnel from performing under the Cooperative Agreement. A major breach of security may occur on or off Government installations, but must be related directly to the work on the Cooperative Agreement. A major breach of security may arise from any of the following: compromise of classified information; illegal technology transfer; workplace violence resulting in criminal conviction; sabotage;

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