

**JSC DATA REQUIREMENTS DESCRIPTION (DRD)**  
(Based on JSC – STD – 123)

<b>1. DRD Title</b> Information Technology Program Security and Reports	<b>2. Version</b> 09/25/2013	<b>3. DRL No.</b> 10	<b>4. RFP/Contract No.</b> NNJ13470997R/ NNJ14HA03B
<b>5. Use (<i>Define need for, intended use of, and/or anticipated results of data</i>)</b> To ensure that IT security reporting requirements are met for all IT systems utilized during work associated with TOs on this contract.			<b>6. DRD Category</b> <input type="checkbox"/> Technical <input checked="" type="checkbox"/> Administrative <input type="checkbox"/> S&MA
<b>6. References</b> NFS 1852.204-76: Security Requirements for Unclassified IT Resources NPR 2810.1(series): Security of Information Technology. OMB Circular A-130: Management of Federal Information Resources	<b>8. Interrelationships (e.g. with other DRDs)</b>		

**A. SCOPE:**

All contracts that purchase, lease, network to, or otherwise utilize Government-funded IT (as defined by the Clinger-Cohen Act of 1996 and referenced by OMB Circular A-130) must comply with NASA IT Security Requirements.

**B. CONTENT:**

**IT SECURITY MANAGEMENT PROGRAM PLAN:**

The Contractor shall submit an IT Security Management Program Plan for its unclassified technology information resources. This program plan shall describe the policy, processes, and procedures that will be followed to ensure appropriate security of IT resources that are developed, processed, or used under this contract. The Contractor's IT Security Management Program Plan shall be compliant with the IT security requirements in accordance with Federal and NASA policies as referenced in OMB Circular A-130 and NPR2810.1(series).

**IT SECURITY PLAN:**

The Contractor shall have Information Systems Security Officer (ISSO) who is responsible for the contractor's system(s) in accordance with the definitions set forth in NPR2810.1(series). The IT security plan shall be kept up to date as changes to the baseline configuration of the system occur and shall be documented in the IT Security Plan. Note: An IT Security Plan is specific to a system or group of systems, while an IT Security Management Program Plan is defined as the elements a contractor has outlined to meet the IT Security requirements for interfacing with other contractors and NASA, training requirements and meeting the requirements in NPR 2810.1(series).

**IT SECURITY AWARENESS TRAINING:**

Employees subject to this contract shall complete the NASA approved IT Security Awareness Training annually. The contractor shall provide evidence that periodic IT security awareness training has been met for all employees subject on this contract. The contractor shall submit periodic reports (as required by the CO) detailing the overall status of the annual training program. The annual training program is defined as the period from October 1st through September 30th.

JSC DATA REQUIREMENTS DESCRIPTION (DRD)  
(Based on JSC – STD – 123)

**IT SECURITY ROLE BASED TRAINING:**

Employees subject to this contract shall complete NASA approved IT Security Training annually related to the following Role Based functions:

- IT Security Manager
- Information System Owner (ISO)
- Information Systems Security Officer (ISSO)
- Organizational Computer Security Official – Representative (OCSO-R)

The contractor shall provide evidence that periodic IT security training has been met for all employees subject on this contract. The contractor shall submit periodic reports (as required by the CO) detailing the overall status of the annual training program. The annual training program is defined as the period from October 1st through September 30th.

**INFORMATION ON EMPLOYEES IN SENSITIVE POSITIONS/ASSIGNMENTS REPORT:**

The Information on Employees is Sensitive. ITS Positions/Assignments Report shall provide information annually for personnel screening as required by NPR 2810.1(series), and NPR 1600.1 on position risk.

**IT POINT OF CONTACT:**

The contractor shall identify a point of contact that NASA may reach in its attempt to address IT and IT Security issues. The point of contact shall have the authority to ensure appropriate actions occur.

**C. FORMAT:**

Contractor's format is acceptable. The plan reports shall be delivered in native format and be compatible with JSC standard software loads.

**D. MAINTENANCE:**

The plan shall be reviewed by the contractor annually and updated as needed or as directed by the contracting officer.

**E. SUBMISSION AND DISTRIBUTION:**

Submission and distribution shall be in accordance with Attachment J-01, Data Requirements List.