

JSC DATA REQUIREMENTS LIST (DRL)

(See reverse for instructions)

a. Title of Contract, Project, SOW, etc.
Occupational Medicine and Occupational Health Contract

b. RFP/Contract No.. NNJ05064093R/NNJ05HA
c. DRL Date/Mod Date

1. Line	2. DRD Title	3. Data <input type="checkbox"/> (1) Written <input checked="" type="checkbox"/> (2) Mandatory Submittal <input type="checkbox"/> (3) Submitted upon	4.	5. As-of-	6. 1 st subm. Award+1mo	7. Copies a. P/E b.
17	Monthly Safety and Health Metrics		MO	10		2
	8. Distribution (Continue on a blank sheet if needed) NS2/Occupational Safety Branch SD3/COTR		9. Remarks			
18	Safety and Health Program Self Evaluation	X <input type="checkbox"/> (1) Written <input checked="" type="checkbox"/> (2) Mandatory Submittal <input type="checkbox"/> (3) Submitted upon	AN	9/30	See #9	4
	8. Distribution (Continue on a blank sheet if needed) NS/Safety and Test Operations Division SD13/Occupational Health Officer JA131/Environmental Services SD3/COTR		9. Remarks Report due September 30 th of each year. System Safety Plan will be required if any facility or operation falls under the applicable requirements of JSC system safety plan as defined in JHB 1700.1H.			
19	System Safety Program Plan	<input type="checkbox"/> (1) Written <input checked="" type="checkbox"/> (2) Mandatory Submittal <input type="checkbox"/> (3) Submitted upon	AN	9/30	See #9	1
	8. Distribution (Continue on a blank sheet if needed) SD3/COTR		9. Remarks Report due September 30 th of each year. System Safety Plan will be required if any facility or operation falls under the applicable requirements of JSC system safety plan as defined in JHB 1700.1H.			
20	Contractor Information Technology Security Management Plan	<input type="checkbox"/> (1) Written <input checked="" type="checkbox"/> (2) Mandatory Submittal <input type="checkbox"/> (3) Submitted upon	AN	11/1	See #9	3
	8. Distribution (Continue on a blank sheet if needed) SA/IT System Administrator SD3/COTR BH4/Contracting Officer and BH 4/Contract Specialist		9. Remarks Draft due at contract start with: final approved by government at contract start + 30 days; annual updates thereafter			

1. DRD Title	2. Date of current version	3. DRL Line Item	RFP/Contract No.
Contractor Information Technology Security Management Plan	12/2004	20	NNJ05064093R/NNJ05HA68C
4. Use <i>(Define need for, intended use of, and/or anticipated results of data)</i> Establishes the policies and procedures to be used by the contractor to maintain information technology security for hardware, software, and data.		5. DRD Category: <i>(check one)</i> Technical <input checked="" type="checkbox"/> Administrative SR&QA	
6. References <i>(Optional)</i>	7. Interrelationships <i>(e.g., with other DRDs) (Optional)</i> See block 8		

8. Preparation Information *(Include complete instructions for document preparation)*

- (a) Description/Use: The plan shall be used to define the contractor IT and computer systems security management. The contractor shall define and describe the approach for assuring the security of medical, technical and otherwise medically sensitive databases and equipment.
- (b) Submission
 - (1) Draft: due at contract start
 - (2) Final shall be approved by the government by contract start + 30 days
 - (3) Submission frequency: annual
- (c) Applicable documents (note: some documents may fall into more than one category and are grouped for reference only)
 - (1) Federal Documents:
 - (i) OMB circular A-130, App. III, Security of Federal Automated Information Resources
 - (ii) NIST Special Publication 800-18 "Guide for Developing Security Plans
 - (iii) FAR 52.204-2
 - (iv) Federal Information Security Management Act (FISMA)
 - (v) Health Insurance Portability and Accountability Act (HIPAA)
 - (2) NASA Agency and JSC Center documents
 - (i) NPR 2810.1 Security of Information Technology
 - (ii) JSC JPG 2810.1B JSC IT Security Handbook
- (d) Data Preparation Information
 - (1) Scope: The Security Management Plan shall describe the Contractor's approach for meeting and maintaining the security integrity of the security baseline. The plan shall address the security requirements for facilities, systems, equipment, personnel, information, communications, and sensitive IT security procedures. This plan establishes the security procedures, Government/contractor relationships and assigns responsibilities for all physical, personnel, and IT security required for the activity specified in the SOW. It is applicable to all contractor and subcontractor personnel, operations and procedures. .
 - (2) Content: The management structure, processes and reporting requirements, techniques and formats shall be established, defined and documented to ensure adequate visibility and insight for Government personnel. The Security Management Plan shall include, as a minimum, the following:
 - (i) A description of the contractor's security management structure and assignment of responsibilities.