ATTACHMENT J-2
IT SECURITY IMPLEMENTATION GUIDE

FOR

MEDICAL AND ENVIRONMENTAL SUPPORT CONTRACT (MESC)

1.1   System and Application Life Cycle Requirements

The contractor shall follow the NIST SP 800-26, Security Self-Assessment Guide for Information Technology Systems, and NIST SP 800-30, Risk Management Guide for Information Technology Systems, requirements during all phases of the System and Application Life Cycle.

1.2   Security Awareness Training

As defined in NPR 2810.1A, all contractor personnel with access to Government data, including off-site personnel supporting the contract shall complete security training annually as required to meet Agency IT security training and awareness requirements. The Contractor shall report quarterly on status of the required training of their employees. Reports shall be submitted to the COTR or designee.

1.3   Security Risk Assessments and Design Reviews

The contractor shall complete a security risk assessment on a design prior to the design being provided to NASA. Before or during official design reviews, the contractor shall provide design security risks, including possible mitigations, to the system owner or data owner and Organization Computer Security Official (OCSO). If the risks are accepted the life cycle may continue; otherwise, the life cycle shall halt or the design and/or mitigations shall be modified until the risks and possible mitigations are acceptable.

1.4   Security Reviews for New or Modified Hardware and Software

The contractor shall provide a written risk assessment and security review for new or significantly modified hardware or software, prior to deployment. The products reviewed shall be used as a basis to update IT Security Plans, as applicable. Prior to deployment, all risks shall be presented to the system owner, Authorizing Official (AO), and OCSO, separate from the security plan. If the hardware or software connects to other systems the risks shall be presented to the system owner or equivalents and OCSO of the interconnected systems for their information.

1.5   Security Training

All contractor individuals who perform tasks as a system administrator, or have authority to perform tasks normally performed by system administrator, shall be required to pass the NASA System Administrator Security Certification.

1.6   System Security Controls for Network Access

Prior to connecting any new non-Government provided computer system or equipment to the KSC Institutional Networks, the contractor shall:

a.   Comply FIPS 199, FIPS 200, and any relevant IT SOPs on certification and accreditation.

b.   Acknowledge all applicable NIST-SP-800-53 controls.

c.   Complete the Privacy Impact Analysis (PIA).

d.   Comply with NPR 2810.1A, IT Security Requirements.

e.   Install and configure Agency Security Update System (ASUS) or approved Agency Patching and Reporting System to Center specifications.

f.   Install and configure Agency Security Configuration Standards (ASCS) to Agency and Center specifications.

g.   Provide a NASA approved Certified System Administrator.

h.   Perform a vulnerability scan, mitigate findings, and document results.

i.   Provide NIST SP-800-53 control acceptance and Plan of Action & Milestones (POA&M) list to be reviewed by the Center's Certification and Accreditation (C&A) Official.

j.   Draft Authorizing Official (AO) letter per NASA Authority to Operate (ATO) process.

k.   Submit the complete package of items a-j above to the Center ITSM for review.

l.   Upon completion of Center ITSM review, submit ATO package to the AO.

1.7   System Security Controls for C&A
For any computer system that is not managed by ODIN or its successor, the contractor shall:

a. Meet the current and future requirements in the NASA-STD-2804, Minimum Interoperability Software Suite, and NASA-STD-2805, Minimum Hardware Configurations, for all computer systems, unless otherwise approved by the COTR.

b. Configure non-NASA managed services desktop systems with the required standard application software suite, if applicable, to stay consistent across the Agency to ensure that interoperability issues do not arise. The Government has defined a core standard application software suite (reference NASA-STD-2804) that is loaded on all NASA managed services computers.

c. Provide and maintain software that is defined in the current and future versions of NASA-STD-2804.

d. Update the computer with new versions, upgrades, modifications, and non-security and non-bug related patches associated with the operation system and application software within 1 year of the latest release by the software vendor or by the date specified in the current and future versions of NASA-STD-2804.

e. Once the contractor has tested the new release, present the test results and any impacts to associated applications then submit to the CCB in sufficient time to ensure roll out within 1 year of release or by the date specified in NASA-STD-2804, unless otherwise specified by the COTR or designee.

f. Configure regular virus scans on all computer systems which the contractor is responsible.

g. Enable real-time file protection and schedule full virus scans no less frequently than weekly, unless otherwise defined in Center policies or directed by the COTR or designee.

h. Configure automatic updates of virus signatures no less frequently than daily for desktops, unless otherwise defined in Center policies or directed by the COTR or designee.

i. Configure, in addition to NASA-STD-2804, regular adware, spyware, and malware scans on all systems for which they are responsible, but not including servers. The contractor shall enable real-time system protection and schedule full adware and spyware scans no less frequently than weekly for any desktops, unless otherwise defined in Center policies.

1.8   Management Controls
The contractor shall provide management control services to implement IT security for MESC at KSC.

In performance of these services, the contractor shall:

a. Participate in the Center-wide vulnerability scanning activity. The contractor shall mitigate vulnerabilities identified, track vulnerabilities and fixes, and report the statistics to the system owner, OCSO, and COTR or designee.

b. Obtain approval from the system owner, OCSO, and COTR for a temporary mitigation. For a medium or low vulnerability, the contractor may mitigate the vulnerability or present a researched recommendation that justifies accepting the risk.

c. Evaluate, test, and implement mitigation of these services; depending on the assessed severity (critical, high, medium, or low) of a vulnerability and system owner, OCSO, and COTR concurrence with the severity.

d. Comply with the standard and expedited requirements in the Vulnerability Mitigation Requirements Table below.

e. Notify the system owner, OCSO, and COTR when the vulnerability is mitigated and steps taken to mitigate the vulnerability.

f. Obtain approval by the system owner, OCSO, and COTR for any deviation from the requirements.

g. Submit a statistics report on a monthly basis for all vulnerabilities mitigated with their associated severity. A permanent mitigation is required for a critical or a

high vulnerability; though in some cases a temporary mitigation may be necessary.

For High Categorization Systems:

STANDARD REQUIREMENT	CRITICAL	HIGH	MEDIUM	LOW
Time to mitigation after severity concurrence	1 business days	5 business days	1 calendar months	Per mitigation plan
Time to create a plan for permanent mitigation	If temporary mitigation is used, 5 business days	If temporary mitigation is used, 15 business days	N/A	3 calendar months
Occurrences expected per contract year	**2**	**20**	**25**	**25**
EXPEDITED REQUIREMENT	**CRITICAL**	**HIGH**	**MEDIUM**	**LOW**
Time to mitigation after severity concurrence	4 business hours	16 business hours	10 business days	N/A
Time to create a plan for permanent mitigation	If temporary mitigation is used, 8 business hours	If temporary mitigation is used, 2 business days	N/A	N/A
Occurrences expected per contract year	1	3	N/A	N/A

For Moderate Categorization Systems:

STANDARD REQUIREMENT	CRITICAL	HIGH	MEDIUM	LOW
Time to mitigation after severity concurrence	5 business days	15 business days	3 calendar months	Per mitigation plan
Time to create a plan for permanent mitigation	If temporary mitigation is used, 10 business days	If temporary mitigation is used, 30 business days	N/A	6 calendar months
Occurrences	**2**	**20**	**25**	**25**

EXPEDITED REQUIREMENT	CRITICAL	HIGH	MEDIUM	LOW
expected per contract year				
Time to mitigation after severity concurrence	4 business hours	16 business hours	10 business days	N/A
Time to create a plan for permanent mitigation	If temporary mitigation is used, 8 business hours	If temporary mitigation is used, 2 business days	N/A	N/A
Occurrences expected per contract year	1	3	N/A	N/A

For Low Categorization Systems:

STANDARD REQUIREMENT	CRITICAL	HIGH	MEDIUM	LOW
Time to mitigation after severity concurrence	5 business days	1 calendar month	Per mitigation plan	Per mitigation plan
Time to create a plan for permanent mitigation	If temporary mitigation is used, 10 business days	If temporary mitigation is used, 30 business days	1 calendar year	1 calendar year
Occurrences expected per contract year	**2**	**20**	**25**	**25**
EXPEDITED REQUIREMENT	**CRITICAL**	**HIGH**	**MEDIUM**	**LOW**
Time to mitigation after severity concurrence	1 business day	5 business days	N/A	N/A
Time to create a plan for permanent mitigation	If temporary mitigation is used, 8 business hours	If temporary mitigation is used, 2 business days	N/A	N/A
Occurrences expected per contract year	1	3	N/A	N/A

1.9   Operational Controls

System Contingency Planning and Emergency Preparedness
In addition to what is stated in NPR 2810.1A, the contractor shall participate in contingency and Disaster Recovery (DR) planning, training, and testing in accordance with the current Center Contingency Plan.

In performance of these services, the contractor shall:

   a. At least annually train contingency teams in plan procedures and operations.

   b. At least annually develop, plan, and implement a contingency scenario test designed to validate the effectiveness of the plan to quickly restore IT operations in the event of a disaster.

   c. Assess lessons learned from each test and use the results to update the IT Contingency Plan.

   d. Participate in Center DR operations, in the event the Center's plan is invoked, in accordance with the Center Contingency and DR Plan.

System Monitoring
In performance of these services, the contractor shall:

   a. Perform all necessary support in the event of a Government-initiated investigation, assessment, or certification involving the contractor's team or the contractor's customers.

   b. Perform all services necessary to properly respond to NASA IT security bulletins or notices from the NASA Incident Response Center (NASIRC), or the NASA Chief Information Officer (CIO) that apply to any contractor-supported system or environment.

   c. Take necessary and/or immediate corrective actions on any system in response to these bulletins and notices, and notify the system owner, COTR, and OCSO of any suspicious activities per Center security procedures.

1.10   IT Security Reporting Requirements
The contractor shall comply with reporting requirements set by the Federal Information Security Management Act (FISMA), the Office of Management and Budget (OMB), the Office of the Inspector General (OIG), and the Center and Agency CIO.

In performance of these services, the contractor shall:

   a. Report IT security incidents to the ITSM or designee(s) within one hour and shall follow the Center's documented IT security incident response procedures.

   b. Report using the format and content set forth in each Center's incident response report (Institutional Security Status).

c. Report unexplained system anomalies that, in the judgment of the system administrator, may affect confidentiality of data or integrity of a system/data to the ITSM or designee within one hour. Such anomalies include, but are not limited to, unexplained change of directory or file permissions, unexplained installation, removal or starting/stopping of software, unexplained network traffic, unexplained unavailability of a production service, or any malicious activity.

d. Provide all necessary assistance to the investigating team.

1.11   Distribution of Risks, Threats and Vulnerabilities
The contractor shall encrypt all electronic transmissions and storage of sensitive but unclassified (SBU) information with the Agency approved encryption software.

1.12   Storage of System Documentation and Backup Media
The contractor shall store duplicate copies of system documentation with the backup media, including updates at an off-site location secure from threats, in accordance the approved security plan.

1.13   Prohibition of Production Data on Non-Production Networks
The contractor shall not store, copy, or transfer NASA SBU data to any non-C&A system, in accordance with NPR 2810.1A or for non-NASA system in accordance with NIST 800-37.