

ORDER FOR SUPPLIES OR SERVICES

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

BPA NO.

1. DATE OF ORDER SEP 17 2010		2. CONTRACT NO. (If any) NNG07DA47B		6. SHIP TO:	
3. ORDER NO. NRC-DR-33-10-359		4. REQUISITION/REFERENCE NO.		a. NAME OF CONSIGNEE NRC Warehouse Facility	
5. ISSUING OFFICE (Address correspondence to) U.S. Nuclear Regulatory Commission Div. of Contracts Attn: Pearlette Merriweather Mail Stop: TWB-01-B10M Rockville MD 20852				b. STREET ADDRESS Attn: Chris Bajwa/Mail Stop EBB3D02M 5008 Broiling Brook Parkway	
7. TO:		c. CITY Rockville	d. STATE MD	e. ZIP CODE 20852	
a. NAME OF CONTRACTOR MICROTECHNOLOGIES LLC MICROTECH				f. SHIP VIA	
b. COMPANY NAME				8. TYPE OF ORDER	
c. STREET ADDRESS 8330 BOONE BLVD STE 600				<input type="checkbox"/> a. PURCHASE <input checked="" type="checkbox"/> b. DELIVERY REFERENCE YOUR Except for billing instructions on the reverse, this Please furnish the following on the terms and delivery order is subject to instructions conditions specified on both sides of this order contained on this side only of this form and is and on the attached sheet, if any, including issued subject to the terms and conditions delivery as indicated. of the above-numbered contract.	
d. CITY VIENNA		e. STATE VA	f. ZIP CODE 221822659		
9. ACCOUNTING AND APPROPRIATION DATA Obligate \$48,159.60 B&R: 010-15-5F1-325 JC: J1267 BOC: 252A APP: 31X0200.010 FSS:10070760 DUNS: 145454182				10. REQUISITIONING OFFICE OIS	

11. BUSINESS CLASSIFICATION (Check appropriate box(es))					12. F.O.B. POINT N/A
<input checked="" type="checkbox"/> a. SMALL	<input type="checkbox"/> b. OTHER THAN SMALL	<input type="checkbox"/> c. DISADVANTAGED	<input checked="" type="checkbox"/> g. SERVICE-DISABLED VETERAN-OWNED		
<input type="checkbox"/> d. WOMEN-OWNED	<input type="checkbox"/> e. HUBZone	<input type="checkbox"/> f. EMERGING SMALL BUSINESS			
13. PLACE OF		14. GOVERNMENT B/L NO.	15. DELIVER TO F.O.B. POINT ON OR BEFORE (Date) DESTINATION		16. DISCOUNT TERMS 30 NET
a. INSPECTION SEE BLOCK 6	b. ACCEPTANCE SEE BLOCK 6				

17. SCHEDULE (See reverse for Rejections)

ITEM NO. (a)	SUPPLIES OR SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
001	Part No. COL2030ARNRC - 10020208- GoToMeeting Seat Renewal		EA			
002	Part No. COL2030NNRC-10020209-GoToMeeting New Seats		EA			
003	SEWP Fee		LT			
The period of performance is 9/29/2010 - 9/28/2011.						

18. SHIPPING POINT		19. GROSS SHIPPING WEIGHT		20. INVOICE NO.		\$48,159.60	17(h) TOTAL (Cont. pages)	
21. MAIL INVOICE TO:								
SEE BILLING INSTRUCTIONS ON REVERSE	a. NAME Department of Interior / NBC NRCPayments@nbc.gov						\$48,159.60	17(i). GRAND TOTAL
	b. STREET ADDRESS (or P.O. Box) Attn: Fiscal Services Branch - D2770 7301 W. Mansfield Avenue							
	c. CITY Denver	d. STATE CO	e. ZIP CODE 80235-2230					

22. UNITED STATES OF AMERICA BY (Signature) <i>Pearlette Merriweather</i>				23. NAME (Typed) Pearlette Merriweather Contracting Officer TITLE: CONTRACTING/ORDERING OFFICER			
---	--	--	--	--	--	--	--

A.1 REQUIREMENT

Statement of Work for Office of Information Services Virtual Meeting Pilot Project August 26, 2010

I. BACKGROUND

After consultation with the Office of Information Services (OIS) and the Computer Security Office (CSO), OEDO initiated a pilot project to provide virtual meeting services to NRC staff in September, 2008. This service would provide two types of virtual meetings:

- Meetings: permits up to 25 connections
- Webinars: permits many more connections up to 1000

Meetings must be used for official NRC business, and meeting participants are subject to all applicable NRC rules and regulations regarding use of government computers, staff conduct and all NRC records and information security rules.

Although the virtual meeting service contract will be co-administered by OHR and OIS, meeting requesters/organizers are responsible for managing meeting logistics. Meetings are scheduled on a first come, first served basis. Offices which have ongoing need will be assigned a virtual meeting license on a "permanent" basis and will be responsible for overseeing use of the license assigned to them.

II. PURPOSE:

To obtain Virtual Meeting Services for use in an extended pilot program for virtual meeting services with the ability to purchase additional licenses at any time before the expiration of the task order. The individual license costs are prorated for the remainder of the government fiscal year and these additional licenses expire at the same time as the original licenses (at the end of the government fiscal year).

III. SERVICE REQUIREMENTS

Objectives for these services will include, at a minimum:

1. Provide virtual meeting services for both meetings and webinar configurations
2. Provide both desktop sharing and audio conferencing options
3. Provide a finite number of licenses (**between 20 and 100**) for use by NRC staff
4. Permit passage of presenter controls from person to person
5. Allow NRC to monitor participant activity including attendees and to the extent possible the activity level of these attendees. Keep track of who is on the call in real time.
6. Enable the meeting organizer/host to actively acknowledge or respond to participant questions in either configuration
7. Permit and facilitate recording of meetings.
8. Provide NRC with **full control** of each session, i.e. control and access to the meeting space
9. Provide technical support during meetings on request
10. Offerors should understand that the NRC Computer Security Office requires that the solution provide complete session confidentiality, communications protection (encryption), full session

- control, security certification and accreditation (which would be needed for both the pilot and any potential follow-on production capability)
11. Offerors should also meet the security requirements provided in the attachment to this Statement of Objectives.

NRC's Draft Information Technology Security Requirements as of July 20, 2009 follow. Offerors should explicitly state in their proposal whether or not their product meets the appropriate portions of the requirements.

1.0 NRC Information Technology Security Requirements

General Requirements - This section provides IT security requirements that must be incorporated into any contract that includes information technology (IT), whether the IT is used for word processing or whether the contract is to develop a new IT system, with the following exceptions: COTS software purchases, hardware purchases, and bank card purchases.

Basic Contract IT Security Requirements

The contractor agrees to insert terms that conform substantially to the language of the IT security requirements, excluding any reference to the Changes clause of this contract, all subcontracts under this contract.

For unclassified information used for the effort, the contractor shall provide an information security categorization document indicating the sensitivity of the information processed as part of this contract if the information security categorization was not provided in the statement of work. The determination shall be made using NIST SP 800-60 and must be approved by CSO. The NRC contracting officer and project officer shall be notified immediately if the contractor begins to process information at a higher sensitivity level.

If the effort includes use or processing of classified information, the NRC contracting officer and project officer shall be notified immediately if the contractor begins to process information at a more restrictive classification level.

All work under this contract shall comply with the latest version of all applicable guidance and standards. Individual task orders will reference applicable versions of standards or exceptions as necessary. These standards include, but are not limited to, NRC Management Directive 12.5 Automated Information Security Program, and National Institute of Standards and Technology (NIST) guidance and Federal Information Processing Standards (FIPS), and Committee on National Security Systems (CNSS) policy, policy, directives, instructions, and guidance. This information is available at the following links:

NRC Policies, Procedures and Standards (CSO internal website):

<http://www.internal.nrc.gov/CSO/policies.html>

All NRC Management Directives (public website):

<http://www.nrc.gov/reading-rm/doc-collections/management-directives/>

NIST SP and FIPS documentation is located at:

<http://csrc.nist.gov/>

CNSS documents are located at:

<http://www.cnss.gov/>

When e-mail is used, the Contractors shall only use NRC provided e-mail accounts to send and receive sensitive information (information that is not releasable to the public) or mechanisms to protect the information during transmission to NRC that have been approved by CSO.

All Contractor employees must sign the NRC Agency Rules of Behavior for Secure Computer Use prior to being granted access to NRC computing resources.

Contractor shall adhere to NRC policies, including but not limited to:

- Management Directive 12.5, Automated Information Security Program
- Computer Security Policy for Encryption of Data at Rest When Outside of Agency Facilities
- Policy for Copying, Scanning, Printing, and Faxing SGI & Classified Information
- Computer Security Information Protection Policy
- Remote Access Policy
- Use of Commercial Wireless Devices, Services and Technologies Policy
- Laptop Security Policy
- Computer Security Incident Response Policy

Contractor will adhere to NRC's prohibition of use of personal devices to process and store NRC sensitive information.

All work performed at non-NRC facilities shall be in facilities, networks, and computers that have been accredited by NRC for processing information at the sensitivity level of the information being processed.

Contract Performance and Closeout

The contractor shall ensure that the NRC data processed during the performance of this contract shall be purged from all data storage components of the contractor's computer facility, and the contractor will retain no NRC data within 30 calendar days after contract is completion. Until all data is purged, the contractor shall ensure that any NRC data remaining in any storage component will be protected to prevent unauthorized disclosure.

When contractor employees no longer require access to an NRC system, the contractor shall notify the project officer within 24 hours.

Upon contract completion, the contractor shall provide a status list of all NRC system users and shall note if any users still require access to the system to perform work if a follow-on contract or task order has been approved by NRC.

Control of Information and Data

The contractor shall not publish or disclose in any manner, without the contracting officer's written consent, the details of any security controls or countermeasures either designed or developed by the contractor under this contract or otherwise provided by the NRC.

Any IT system used to process NRC sensitive information shall:

- Include a mechanism to require users to uniquely identify themselves to the system before beginning to perform any other actions that the system is expected to provide.
- Be able to authenticate data that includes information for verifying the claimed identity of individual users (e.g., passwords)
- Protect authentication data so that it cannot be accessed by any unauthorized user
- Be able to enforce individual accountability by providing the capability to uniquely identify each individual computer system user
- Report to appropriate security personnel when attempts are made to guess the authentication data whether inadvertently or deliberately

Access Controls

Any contractor system being used to process NRC data shall be able to define and enforce access privileges for individual users. The discretionary access controls mechanisms shall be configurable to protect objects (e.g., files, folders) from unauthorized access.

The contractor system being used to process NRC data shall provide only essential capabilities and specifically prohibit and/or restrict the use of specified functions, ports, protocols, and/or services.

The contractors shall only use NRC approved methods to send and receive information considered sensitive or classified. Specifically,

- **Classified Information** - All NRC Classified data being transmitted over a network shall use NSA approved encryption and adhere to guidance in MD 12.2 NRC Classified Information Security Program, MD 12.5 NRC Automated Information Security Program and Committee on National Security Systems. Classified processing shall be only within facilities, computers, and spaces that have been specifically approved for classified processing.
- **SIGINT Information** – All SIGINT being transmitted over a network shall adhere to guidance in MD 12.7 NRC Safeguards Information Security Program and MD 12.5 NRC Automated Information Security Program. SIGINT processing shall be only within facilities, computers, and spaces that have been specifically approved for SIGINT processing. Cryptographic modules provided as part of the system shall be validated under the Cryptographic Module Validation Program to conform to NIST FIPS 140-2 overall level 2 and must be operated in FIPS mode. The contractor shall provide the FIPS 140-2 cryptographic module certificate number and a brief description of the encryption module that includes the encryption algorithm(s) used, the key length, and the vendor of the product.

The most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks must be enforced by the system through assigned access authorizations.

Separation of duties for contractor systems used to process NRC information must be enforced by the system through assigned access authorizations. The mechanisms within the contractor system or application that enforces access control and other security features shall be continuously protected against tampering and/or unauthorized changes.

Configuration Standards

All systems used to process NRC sensitive information shall meet NRC configuration standards available at: <http://www.internal.nrc.gov/CSO/standards.html>.

Information Security Training and Awareness Training

Contractors shall ensure that their employees, consultants, and subcontractors that have significant IT responsibilities (e.g. IT administrators, developers, project leads) receive in-depth IT security training in their area of responsibility. This training is at the employer's expense.

Media Handling

All media used by the contractor to store or process NRC information shall be controlled in accordance to the sensitivity level. The contractor shall not perform sanitization or destruction of media approved for processing NRC information designated as SIGINT or Classified. The contractor must provide the media to NRC for destruction.

Vulnerability Management

The Contractor must adhere to NRC patch management processes for all systems used to process NRC information. Patch Management reports will be made available to the NRC upon request for following security categorizations and reporting timeframes:

- 5 calendar days after being requested for a high sensitivity system
- 10 calendar days after being requested for a moderate sensitivity system
- 15 calendar days after being requested for a low sensitivity system

For any contractor system used to process NRC information, the contractor must ensure that information loaded into the system is scanned for viruses prior to posting; servers are scanned for viruses, adware, and spyware on a regular basis; and virus signatures are updated at the following frequency:

- 1 calendar day for a high sensitivity system
- 3 calendar days for a moderate sensitivity system
- 7 calendar days for a low sensitivity system

Development and Operations and Maintenance Requirements

These IT security requirements are to be inserted into any contract that includes IT system development or operations and maintenance activities. Information system resources include, but are not limited to, hardware, application software, system software, and information (data). Information system services include, but are not limited to, the management, operation (including input, processing, transmission, and output), maintenance, programming, and system administration of computer systems, networks, and telecommunications systems.

O&M Security Requirements

All system modifications to classified systems must comply with NRC security policies and procedures for classified systems, as well as federal laws, guidance, and standards to ensure Federal Information Security Management Act (FISMA) compliance.

The Contractor shall correct errors in contractor developed software and applicable documentation that are not commercial off-the-shelf which are discovered by the NRC or the contractor. Inability of the parties to determine the cause of software errors shall be resolved in accordance with the Disputes clause in Section I, FAR 52.233-1, incorporated by reference in the contract.

The Contractor shall adhere to the guidance outlined in NIST SP 800-53, FIPS 200 and NRC guidance for the identification and documentation of minimum security controls.

The contractor shall provide the system requirements traceability matrix at the end of the initiation phase, development/acquisition phase, implementation/assessment phase, operation & maintenance phase and disposal phase that provides the security requirements in a separate section so that they can be traced through the development life cycle. The contractor shall also provide the software and hardware designs and test plan documentation, and source code upon request to the NRC for review.

All development and testing of the systems shall be protected at their assigned system sensitivity level and shall be performed on a network separate and isolated from the NRC operational network.

All system computers must be properly configured and hardened according to NRC policies, guidance, and standards and comply with all NRC security policies and procedures as commensurate with the system security categorization.

All contractor provided deliverables identified in the project plan will be subject to the review and approval of NRC Management. The contractor will make the necessary modifications to project deliverables to resolve any identified issues. Project deliverables include but are not limited to: requirements, architectures, design documents, test plans, and test reports.

Access controls

The contractor shall not hardcode any passwords into the software unless the password only appears on the server side (e.g. using server-side technology such as ASP, PHP, or JSP).

The contractor shall ensure that the software does not contain undocumented functions and undocumented methods for gaining access to the software or to the computer system on which it is installed. This includes, but is not limited to, master access keys, back doors, or trapdoors.

Cryptography

Cryptographic modules provided as part of the system shall be validated under the Cryptographic Module Validation Program to conform to NIST FIPS 140-2 and must be operated in FIPS mode. The contractor shall

provide the FIPS 140-2 cryptographic module certificate number and a brief description of the encryption module that includes the encryption algorithm(s) used, the key length, and the vendor of the product.

Configuration Management and Control

The contractor must ensure that the system will be divided into configuration items (CIs). CIs are parts of a system that can be individually managed and versioned. The system shall be managed at the CI level. The contractor must have a configuration management plan that includes all hardware and software that is part of the system and contains at minimum the following sections:

- a. Introduction
 - i. Purpose & Scope
 - ii. Definitions
 - iii. References
- b. Configuration Management
 - i. Organization
 - ii. Responsibilities
 - iii. Tools and Infrastructure
- c. Configuration Management Activities
 - i. Specification Identification
 - ii. Change control form identification
 - iii. Project baselines
- d. Configuration and Change Control
 - i. Change Request Processing and Approval
 - ii. Change Control Board
- e. Milestones
 - i. Define baselines, reviews, audits
- f. Training and Resources

The Information System Security Officer's (ISSO's) role in the change management process must be described. The ISSO is responsible for the security posture of the system. Any changes to the system security posture must be approved by the ISSO. The contractor should not have the ability to make changes to the system's security posture without the appropriate involvement and approval of the ISSO.

The contractor shall track and record information specific to proposed and approved changes that minimally include:

- a. Identified configuration change
- b. Testing of the configuration change
- c. Scheduled implementation the configuration change
- d. Track system impact of the configuration change
- e. Track the implementation of the configuration change
- f. Recording & reporting of configuration change to the appropriate party
- g. Back out/Fall back plan
- h. Weekly Change Reports and meeting minutes
- i. Emergency change procedures
- j. List of team members from key functional areas

The contractor shall provide a list of software and hardware changes in advance of placing them into operation within the following timeframes:

- 30 calendar days for a classified, SGI, or high sensitivity system
- 20 calendar days for a moderate sensitivity system
- 10 calendar days for a low sensitivity system

The contractor must maintain all system documentation that is current to within:

- 10 calendar days for a classified, SGI, or high-sensitivity system
- 20 calendar days for a moderate sensitivity system
- 30 calendar days for a low sensitivity system

Modified code, tests performed and test results, issue resolution documentation, and updated system documentation shall be deliverables on the contract. Any proposed changes to the system must have written approval from the NRC project officer.

The contractor shall maintain a list of hardware, firmware and software changes that is current to within:

- 15 calendar days for a classified, SGI or high sensitivity system
- 20 calendar days for a moderate sensitivity system
- 30 calendar days for a low sensitivity system

The contractor shall analyze proposed hardware and software configurations and modification as well as addressed security vulnerabilities in advance of NRC accepted operational deployment dates within:

- 15 calendar days for a classified, SGI, or high sensitivity system
- 20 calendar days for a moderate sensitivity system
- 30 calendar days for a low sensitivity system

The contractor shall provide the above analysis with the proposed hardware and software for NRC testing in advance of NRC accepted operational deployment dates within:

- 15 calendar days for a classified, SGI, or high sensitivity system
- 20 calendar days for a moderate sensitivity system
- 30 calendar days for a low sensitivity system

Control of Hardware and Software

The contractor shall demonstrate that all hardware and software meet security requirements prior to being placed into the NRC production environment.

The contractor shall ensure that the development environment is separated from the operational environment using NRC CSO approved controls.

The contractor shall only use licensed software and in-house developed authorized software (including NRC and contractor developed) on the system and for processing NRC information. Public domain, shareware, or freeware shall only be installed after prior written approval is obtained from the NRC Chief Information Security Officer (CISO).

The contractor shall provide proof of valid software licensing upon request of the Contracting Officer, the NRC Project Officer, a Senior Information Technology Security Officer (SITSO), or the Designated Approving Authorities (DAAs).

Information Security Training and Awareness Training

The contractor shall ensure that its employees, in performance of the contract, receive Information Technology (IT) security training in their role at the contractor's expense. The Contractor must provide the NRC written certification that training is complete, along with the title of the course and dates of training as a prerequisite to start of work on the contract.

The IT security role and associated type of training course and periodicity required to be completed are as follows:

Role	Type of Training	Required Frequency of Training
Auditor	Vendor specific operating system and application security training, database security training	Prior to appointment and then every three years
IT Functional Manager	Vendor specific operating system and application security training, database security training	Prior to appointment and then every two years Additional system specific training upon a major system update/change
System Administrator	Vendor specific operating system and application security training	Prior to appointment and then every year: <ul style="list-style-type: none"> • Training in operating system security in the area of responsibility occurs every 2 years • Training in application security in the area of responsibility occurs every 2 years
Information Systems Security Officer	ISSO role specific training (not awareness) provided by a government agency or by a vendor such as SANS Vendor specific operating system and application security training	Prior to appointment and then every year: <ul style="list-style-type: none"> • Training in the ISSO role occurs every 3 years • Training in operating system security in the area of responsibility occurs every 3 years • Training in application security in the area of responsibility occurs every 3 years
Database Administrator	Vendor specific database security training	Prior to appointment and then every 2 years: <ul style="list-style-type: none"> • Training in database security in the area of responsibility occurs every 2 years
Network Administrator	Network administrator role specific training (not awareness) provided by a government agency or by a vendor such as SANS Network specific security training	Prior to appointment and then every year: <ul style="list-style-type: none"> • Training in the Network administrator role occurs every 3 years • Training in network security in the area of responsibility occurs every year where network administrator role training does not occur
IT Managers	Vendor specific operating	Prior to appointment and then

Role	Type of Training	Required Frequency of Training
	system and application security training, database security training.	every two years Additional system specific training upon a major system update/change
IT System Developer	Vendor specific operating system and application security training, database security training	Prior to appointment and then every year – training with system-specific training (ISS LoB or commercial) upon assuming the role, to become biannual with NRC provided training every other year.

The contractor must ensure that required refresher training is accomplished in accordance with the required frequency specifically associated with the IT security role.

Auditing

The system shall be able to create, maintain and protect from modification or unauthorized access or destruction an audit trail of accesses to the objects it protects. The audit data shall be protected so that read access to it is limited to those who are authorized.

The system shall be able to record the following types of events: use of identification and authentication mechanisms, introduction of objects into a user's address space (e.g., file open, program initiation), deletion of objects, and actions taken by computer operators and system administrators or system security officers and other security relevant events. The system shall be able to audit any override of security controls.

The Contractor shall ensure auditing is implemented on the following:

- Operating System
- Application
- Web Server
- Web Services
- Network Devices
- Database
- Wireless

The contractor shall perform audit log reviews daily using automated analysis tools.

Contractor must log at least the following events on systems that process NRC information:

- a. Audit all failures
- b. Successful logon attempt
- c. Failure of logon attempt
- d. Permission Changes
- e. Unsuccessful File Access
- f. Creating users & objects
- g. Deletion & modification of system files
- h. Registry Key/Kernel changes
- i. Startup & shutdown

- j. Authentication
- k. Authorization/permission granting
- l. Actions by trusted users
- m. Process invocation
- n. Controlled access to data by individually authenticated user
- o. Unsuccessful data access attempt
- p. Data deletion
- q. Data transfer
- r. Application configuration change
- s. Application of confidentiality or integrity labels to data
- t. Override or modification of data labels or markings
- u. Output to removable media
- v. Output to a printer

Contractor Facilities

This section provides IT security requirements that must be incorporated into any contract that includes information technology (IT) activities at a contractor facility. The security requirements to be included in these contracts are provided below.

Backups

Contractor shall ensure that backup media is created, encrypted (in accordance with information sensitivity) and verified to ensure that data can be retrieved and is restorable to NRC systems based on information sensitivity levels. Backups shall be executed to create readable media to which allows successful file/data restoration at the following frequencies:

- At least every 1 calendar day for a high sensitivity system
- At least every 1 calendar day for a moderate sensitivity system
- At least every 7 calendar days for a low sensitivity system

Perimeter Protection

The Contractor must employ perimeter protection mechanisms, such as firewalls and routers, to deny all communications unless explicitly allowed by exception.

Contractor must deploy and monitor intrusion detection capability and have an always deployed and actively engaged security monitoring capability in place for systems placed in operation for the NRC. Intrusion detection and monitoring reports will be made available to the NRC upon request for following security categorizations and reporting timeframes:

- 5 calendar days after being requested for a high sensitivity system
- 10 calendar days after being requested for a moderate sensitivity system
- 15 calendar days after being requested for a low sensitivity system

Certification and Accreditation Security Requirements

The following IT security requirements are to be inserted into any contract that may perform certification and accreditation activities.

Security Risk Assessment

The contractor shall work with the NRC project officer in performing Risk Assessment activities according to NRC policy, standards, and guidance. The contractor shall perform Risk Assessment activities that include analyzing how the architecture implements the NRC documented security policy for the system, assessing how management, operational, and technical security control features are planned or implemented and how the system interconnects to other systems or networks while maintaining security.

System Security Plan

The contractor shall develop the system security plan (SSP) according to NRC policy, standards, and guidance to define the implementation of IT security controls necessary to meet both the functional assurance and security requirements. The contractor will ensure that all controls required to be implemented are documented in the SSP.

Assessment Procedures – Security Test & Evaluation

The contractor shall follow NRC policy, standards, and guidance for execution of the test procedures. These procedures shall be supplemented and augmented by tailored test procedures based on the control objective as it applies to NRC. The contractor shall include verification and validation to ensure that appropriate corrective action was taken on identified security weaknesses.

The contractor shall perform ST&E activities, including but not limited to, coordinating the ST&E and developing the ST&E Plan, execution ST&E test cases and documentation of test results. The contractor shall prepare the Plan of Action and Milestones (POA&M) based on the ST&E results.

Plan of Action and Milestones (POA&M) Maintenance & Reporting

The contractor shall provide a determination, in a written form agreed to by the NRC project officer and Computer Security Office, on whether the implemented corrective action was adequate to resolve the identified information security weaknesses and provide the reasons for any exceptions or risked-based decisions. The contractor shall document any vulnerabilities indicating which portions of the security control have not been implemented or applied.

The contractor shall develop and implement solutions that provide a means of planning and monitoring corrective actions; define roles and responsibilities for risk mitigation; assist in identifying security funding requirements; track and prioritize resources; and inform decision-makers of progress of open POA&M items. The contractor shall perform verification of IT security weaknesses to ensure that all weaknesses identified through third party (e.g., OIG) audits are included in the POA&Ms that the quarterly reporting to OMB is accurate, and the reasons for any exceptions or risked-based decisions are reasonable and clearly documented. This verification process will be done in conjunction with the continuous monitoring activities.

Certification & Accreditation Documentation

The contractor shall create, update maintain all Certification and Accreditation (C&A) documentation in accordance with the following NRC Certification and Accreditation procedures and guidance:

- C&A Non-SGI Unclassified Systems
- C&A SGI Unclassified Systems
- C&A Classified Systems

Contract must develop contingency plan and ensure annual contingency testing is completed within one year of previous test and provide an updated security plan and test report according to NRC's policy and procedure. Contractor must conduct annual security control testing according to NRC's policy and procedure and update POA&M, SSP, etc. to reflect any findings or changes to management, operational and technical controls.

52.217-5 EVALUATION OF OPTIONS (JUL 1990)

Except when it is determined in accordance with FAR 17.206(b) not to be in the Government's best interests, the Government will evaluate offers for award purposes by adding the total price for all options to the total price for the basic requirement. Evaluation of options will not obligate the Government to exercise the option(s).

2052.215-71 PROJECT OFFICER AUTHORITY (NOVEMBER 2006)

(a) The contracting officer's authorized representative (hereinafter referred to as the project officer) for this contract is:

(b) Performance of the work under this contract is subject to the technical direction of the NRC project officer. The term "technical direction" is defined to include the following:

(1) Technical direction to the contractor which shifts work emphasis between areas of work or tasks, authorizes travel which was unanticipated in the Schedule (i.e., travel not contemplated in the Statement of Work (SOW) or changes to specific travel identified in the SOW), fills in details, or otherwise serves to accomplish the contractual SOW.

(2) Provide advice and guidance to the contractor in the preparation of drawings, specifications, or technical portions of the work description.

(3) Review and, where required by the contract, approval of technical reports, drawings, specifications, and technical information to be delivered by the contractor to the Government under the contract.

(c) Technical direction must be within the general statement of work stated in the contract. The project officer does not have the authority to and may not issue any technical direction which:

(1) Constitutes an assignment of work outside the general scope of the contract.

(2) Constitutes a change as defined in the "Changes" clause of this contract.

(3) In any way causes an increase or decrease in the total estimated contract cost, the fixed fee, if any, or the time required for contract performance.

(4) Changes any of the expressed terms, conditions, or specifications of the contract.

(5) Terminates the contract, settles any claim or dispute arising under the contract, or issues any unilateral directive whatever.

(d) All technical directions must be issued in writing by the project officer or must be confirmed by the project officer in writing within ten (10) working days after verbal issuance. A copy of the written direction must be furnished to the contracting officer. A copy of NRC Form 445, Request for Approval of Official Foreign Travel, which has received final approval from the NRC must be furnished to the contracting officer.

(e) The contractor shall proceed promptly with the performance of technical directions duly issued by the project officer in the manner prescribed by this clause and within the project officer's authority under the provisions of this clause.

(f) If, in the opinion of the contractor, any instruction or direction issued by the project officer is within one of the categories as defined in paragraph (c) of this section, the contractor may not proceed but shall notify the contracting officer in writing within five (5) working days after the receipt of any instruction or direction and shall request the contracting officer to modify the contract accordingly. Upon receiving the notification from the contractor, the contracting officer shall issue an appropriate contract modification or advise the contractor in writing that, in the contracting officer's opinion, the technical direction is within the scope of this article and does not constitute a change under the "Changes" clause.

(g) Any unauthorized commitment or direction issued by the project officer may result in an unnecessary delay in the contractor's performance and may even result in the contractor expending funds for unallowable costs under the contract.

(h) A failure of the parties to agree upon the nature of the instruction or direction or upon the contract action to be taken with respect thereto is subject to 52.233-1 -Disputes.

(i) In addition to providing technical direction as defined in paragraph (b) of the section, the project officer shall:

(1) Monitor the contractor's technical progress, including surveillance and assessment of performance, and recommend to the contracting officer changes in requirements.

(2) Assist the contractor in the resolution of technical problems encountered during performance.

(3) Review all costs requested for reimbursement by the contractor and submit to the contracting officer recommendations for approval, disapproval, or suspension of payment for supplies and services required under this contract.

(4) Assist the contractor in obtaining the badges for the contractor personnel.

(5) Immediately notify the Security Branch, Division of Facilities and Security (SB/DFS) (via e-mail) when a contractor employee no longer requires access authorization and return of any NRC issued badge to SB/DFS within three days after their termination.

(6) Ensure that all contractor employees that require access to classified Restricted Data or National Security Information or matter, access to sensitive unclassified information (Safeguards, Official Use Only, and Proprietary information) access to sensitive IT systems or data, unescorted access to NRC controlled buildings/space, or unescorted access to protected and vital areas of nuclear power plants receive approval of SB/DFS prior to access in accordance with Management Directive and Handbook 12.3.

(7) For contracts for the design, development, maintenance or operation of Privacy Act Systems of Records, obtain from the contractor as part of closeout procedures, written certification that the contractor has returned to NRC, transferred to the successor contractor, or destroyed at the end of the contract in accordance with instructions provided by the NRC Systems Manager for Privacy Act Systems of Records, all records (electronic or paper) which were created, compiled, obtained or maintained under the contract.

Master Subscription Agreement: TERMS AND CONDITIONS

This Master Subscription Agreement is entered into as of the Effective Date, by and between Citrix Online LLC, a Delaware limited liability company and a wholly-owned subsidiary of MicroTechnologies, LLC. ("MicroTech"), and "Customer," as identified on the MSA Order Form. By signing the MSA Order Form, each party certifies that it has read, understands and agrees to the provisions set out in the MSA Order Form and these Terms and Conditions, the combination of which comprises the Master Subscription Agreement (this "Agreement"). The "Effective Date" of this Agreement shall be as stated on the MSA Order Form.

1. Description of Services. Through this agreement the products and services of Citrix Online LLC, a Delaware limited liability company and a wholly-owned subsidiary of Citrix Systems, Inc. ("Citrix Online") are being provided. Citrix Online's remote access service products consist of GoToAssist[®], GoToMeeting[®], GoToWebinar[®], GoToTraining[™], and GoToMyPC[®] (individually and collectively referred to as the "Services"), as more fully described in subsections (a) through (e) immediately below. The MSA Order Form identifies the specific Service(s) subscribed to by Customer and indicates the number of Named Authorized User(s) for each Service. "Named Authorized Users" shall mean (i) for the GoToAssist, GoToMeeting, GoToWebinar and GoToTraining Services, the Customer-designated individuals (i.e., employees, contractors, consultants, etc.) whom may access the Services in accordance with this Agreement, and (ii) for the GoToMyPC Service, the Customer-designated host PCs which may be accessed by authorized individuals (i.e., employees, contractors, consultants, etc.) in accordance with this Agreement. The following describes the Services currently offered by Citrix Online:

a. GoToAssist. By subscribing to the GoToAssist Service, Customer may access and use the GoToAssist screen-sharing application for the sole purpose of enabling Named Authorized Users to provide remote assistance to its internal and external customers.

b. GoToMeeting. By subscribing to the GoToMeeting Service, Customer may access and use the GoToMeeting online meeting application for the sole purpose of conducting online meetings between Named Authorized Users and their respective invited attendees.

c. GoToWebinar. By subscribing to the GoToWebinar Service, Customer may access and use the GoToWebinar web conferencing application for the sole purpose of conducting online Webinars between Named Authorized Users and their respective invited attendees.

d. GoToTraining. By subscribing to the GoToTraining Service, Customer may access and use the

GoToTraining online training application for the sole purpose of conducting online training between Named Authorized Users and their respective invited attendees, which allows synchronous online training sessions, distribution of course materials, testing and assessments, publishing upcoming courses to a catalog, and maintaining a reusable content library.

e. GoToMyPC. By subscribing to the GoToMyPC Service, Customer may access and use the GoToMyPC remote-access screen-sharing application for the sole purpose of enabling authorized individuals to remotely access and control Named Authorized Users.

2. Customer Rights and Restrictions.

a. During the Term of this Agreement, and upon payment of all applicable Fees, Customer may access and use the Services subscribed to hereunder pursuant to and in accordance with the provisions of this Agreement.

b. Citrix Online will enable Named Authorized Users to access and utilize the Services as contemplated herein.

c. In connection with the Services subscribed to hereunder, Citrix Online will make available to Customer remote training session(s) via telephone and the Internet for all individuals whom are either Named Authorized Users or authorized to access Named Authorized Users hereunder.

d. Customer may not reverse engineer, decompile or otherwise attempt to decipher any code in connection with the Services or any other aspect of Citrix Online's technology.

e. Customer may reassign Named Authorized Users without incurring additional fees.

f. Subject to Sections 4 and 9(n), Customer may subscribe to additional Services, including new service offerings as may be made available from time to time, and/or increase the number of Named Authorized Users by providing MicroTech (i) a completed Citrix Online Add-On Order Form, (ii) a Customer-issued purchase order, or (iii) a written amendment to this Agreement signed by both parties.

g. Customer may inform its Named Authorized Users, customers and employees that the Services subscribed to hereunder are powered by Citrix Online.

h. No other rights are granted hereunder except as expressly set forth in this Agreement.

3. Term and Termination. Shall be provided for in the Government Purchase Order.

4. **Fees.** Customer shall pay to MicroTech all Fees as stated on the Government Purchase Order, and written amendment to this Agreement signed by both parties, as applicable, within thirty (30) days of date of invoice.

a. **Description of Fees.** "Fees" shall include the following, as applicable:

i. **Subscription Fee.** The "Subscription Fee" is a fee for Customer's access to and use of each of the Services subscribed to hereunder, and shall be due and payable throughout the Term according to the Billing Frequency selected by Customer as stated on the MSA Order Form.

ii. **Implementation Fee.** The "Implementation Fee" (if any) is a one-time fee for implementation by Citrix Online of the Services and is nonrefundable to Customer unless Citrix Online fails to complete such implementation.

iii. **Option Fee.** The "Option Fee" (if any) is a fee for options available to and selected by Customer to customize and enhance the Services subscribed to hereunder, and shall be due and payable throughout the Term according to the Billing Frequency selected by Customer as stated on the MSA Order Form.

b. **Add-on Services.** At any time and pursuant to Section 2(f), Customer may add additional Named Authorized Users, Services, and/or options by notifying MicroTech in writing at info@microtech.net, providing the documentation listed in subsections (i), (ii), or (iii) of Section 2(f), and paying the additional Fees, as applicable, in accordance with this Section 4, for any such addition.

c. **Late Payments.** Payments of Fees which are due hereunder and not received by Citrix Online on or before the applicable due date will accrue interest from such due date through the date paid at the lesser of the rate of (i) 10% per year or (ii) the highest rate allowed by applicable law.

d. **Taxes and Withholding.** Customer shall be responsible for all applicable taxes (withholding tax, sales tax, services tax, value-added tax (VAT), goods and services tax (GST), etc.) or duties imposed by any government entity or collecting agency EXCEPT those taxes based on Citrix Online's or Citrix Systems, Inc.'s net income.

5. **Confidential Information.** Unless expressly authorized in writing by the other party, neither party shall disclose to any third party any non-public information or materials provided by the other party under this Agreement and reasonably understood to be confidential ("Confidential Information"), or use such Confidential Information in any manner other than to perform its obligations under this Agreement. The foregoing restrictions do not apply to any information that (i) is in or becomes available through the public domain, (ii) is already lawfully in the receiving party's possession, (iii) was known to the receiving party prior to the date of disclosure, (iv) becomes known to the receiving party from a third party having an apparent bona fide right to disclose the information, or (v) Confidential Information that the receiving party is obligated to produce pursuant to an order of a court of competent jurisdiction or a valid administrative

subpoena, providing receiving party provides disclosing party timely notice of such court order or subpoena. Furthermore, Customer will keep in strict confidence all passwords and other access information to the Services.

6. **Representations and Warranties.** Each party hereby represents and warrants to the other party that it has all necessary authority to enter into and perform its obligations under this Agreement without the consent of any third party or breach of any contract or agreement with any third party, and that it shall materially comply with applicable rules, regulations and laws relating to the access to and/or use of the Services. CITRIX ONLINE WARRANTS THAT (i) ANY SERVICES PROVIDED HEREUNDER BY CITRIX ONLINE WILL PERFORM SUBSTANTIALLY IN ACCORDANCE WITH CITRIX ONLINE'S DOCUMENTATION ASSOCIATED WITH SUCH SERVICES. CITRIX ONLINE WILL USE ALL REASONABLE COMMERCIAL EFFORTS TO PROVIDE THE SUPPORT REQUESTED BY CUSTOMER UNDER THIS AGREEMENT IN A PROFESSIONAL AND WORKMANLIKE MANNER, BUT CITRIX ONLINE CANNOT GUARANTEE THAT EVERY QUESTION OR PROBLEM RAISED BY CUSTOMER WILL BE RESOLVED IN A CERTAIN RESOLUTION TIME and (ii) EACH SERVICE, WHEN, AND AS MADE AVAILABLE BY CITRIX ONLINE, DOES NOT CONTAIN ANY VIRUS OR OTHER SOFTWARE ROUTINE DESIGNED TO ERASE, DISABLE, OR OTHERWISE HARM CUSTOMER'S EQUIPMENT, DATA, OR OTHER SOFTWARE. TO THE EXTENT PERMITTED BY APPLICABLE LAW, CITRIX ONLINE MAKES NO OTHER WARRANTY, EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, INCLUDING THOSE OF MERCHANTABILITY, SATISFACTORY QUALITY, TITLE, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. (CITRIX ONLINE OFFERS INFRINGEMENT INDEMNIFICATION IN SECTION 7).

7. **Indemnification.**

a. **Defense or Settlement of Claims.** Subject to Sections 7(b) and 7(c) below, Citrix Online shall hold harmless, indemnify and defend any claim, suit or proceeding brought against a Customer based on an allegation that the Services (excluding open source software), as used by Customer in accordance with this Agreement, infringes upon any patent or any copyright or violates any trade secret rights of any party ("Infringement Claims"), provided Customer promptly notifies Citrix Online in writing of its notification or discovery of an Infringement Claim such that Citrix Online is not prejudiced by any delay of such notification. Citrix Online shall pay reasonable attorney's fees, court costs, and damages finally awarded in such Infringement Claim and the reasonable costs associated with any settlement of any Infringement Claim by Citrix Online. Citrix Online will have sole control over the defense and any settlement of any Infringement Claim, and Customer will provide reasonable assistance in the defense of same. Citrix Online will reimburse Customer for reasonable expenses incurred in providing such assistance. Citrix Online shall not enter into any settlement agreement which conveys any

obligation on Customer without Customer's prior written consent. Customer may participate in the defense or settlement of an Infringement Claim with counsel of its own choice and at its own expense, however, Customer shall not enter into any settlement agreement or otherwise settle any such Infringement Claim without Citrix Online's express prior written consent or request.

b. **Infringement Cures.** Following notice of an Infringement Claim, and in the event an injunction is sought or obtained against use of the Services subscribed to hereunder or in Citrix Online's opinion is likely to be sought or obtained, Citrix Online shall, at its option and expense, either (i) procure for Customer the right to continue to use the Services as contemplated herein, or (ii) replace or modify the Services to make its use non-infringing while being capable of performing the same function without degradation of performance. In the event the options set forth in subsections (i) and (ii) herein above are not reasonably available, Citrix Online may in its sole discretion, upon written notice to Customer, terminate this Agreement, cancel access to the Services and refund to Customer any prepaid, but unused Subscription Fees.

c. **Limitation.** Neither MicroTech nor Citrix Online assume any liability, and shall have no liability, for any Infringement Claim based on (i) Customer's access to and/or use of the Services after notice that Customer should cease use of such Services due to an Infringement Claim; (ii) any unauthorized modification of the Services by Customer or at its direction; (iii) Customer's unauthorized combination of the Services with third party programs, data, hardware, or other materials; or (iv) any trademark infringement involving any marking or branding not applied by Citrix Online or involving any marking or branding applied at Customer's request.

d. THE FOREGOING STATES THE EXCLUSIVE REMEDY OF CUSTOMER WITH RESPECT TO ANY INFRINGEMENT CLAIM.

8. **LIMITATION ON LIABILITY.** EXCEPT FOR (i) CITRIX ONLINE'S INDEMNIFICATION OBLIGATION UNDER SECTION 7, (ii) A BREACH BY CUSTOMER OF SECTION 2(d), or (iii) EITHER PARTY'S BREACH OF SECTION 5, AND TO THE EXTENT REQUIRED BY APPLICABLE LAW:

a. THE TOTAL CUMULATIVE LIABILITY OF EITHER PARTY, THEIR RESPECTIVE LICENSORS AND SUPPLIERS ARISING OUT OF THIS AGREEMENT AND/OR THE TERMINATION THEREOF SHALL BE LIMITED TO THE SUM OF THE AMOUNTS PAID AND OWING DURING THE TERM OF THIS AGREEMENT; and

b. NEITHER PARTY SHALL BE LIABLE TO THE OTHER OR ANY OTHER PERSON FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL OR INCIDENTAL, MULTIPLE, PUNITIVE OR OTHER DAMAGES (INCLUDING, WITHOUT LIMITATION, LOSS OF DATA, LOSS OF INCOME, LOSS OF OPPORTUNITY, LOST PROFITS, COSTS OF RECOVERY OR ANY OTHER DAMAGES), HOWEVER CAUSED AND BASED ON ANY

THEORY OF LIABILITY, AND WHETHER OR NOT FOR BREACH OF CONTRACT, NEGLIGENCE, OR OTHERWISE, AND WHETHER OR NOT SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

9. **Additional Terms.**

a. **Assignment.** Customer may not assign its rights or delegate its duties under this Agreement either in whole or in part without the prior written consent of Citrix Online (which consent shall not be unreasonably withheld), except that Customer may assign this Agreement in whole as part of a corporate reorganization, consolidation, merger, or sale of substantially all of its assets. Any attempted assignment or delegation without such consent shall be void. This Agreement will bind and inure to the benefit of each party's successors and permitted assigns.

b. **Force Majeure.** Neither party will be responsible for any delay, interruption or other failure to perform under this Agreement due to acts beyond the control of the responsible party, but only for so long as such conditions persist. Force majeure events include, but are not limited to: natural disasters (e.g., lightning, earthquakes, hurricanes, floods); wars, riots, terrorist activities, and civil commotions; activities of local exchange carriers, telephone carriers, Internet service providers, and other third parties; explosions and fires; embargoes, strikes, and labor disputes; governmental decrees; and any other cause beyond the reasonable control of a party.

c. **Choice of Law.** This Agreement and any dispute arising out of or in connection with this Agreement shall be governed by and construed under the laws of the State of Florida, without regard to the principles of conflict of laws.

d. **Notice.** Any and all notices required under this Agreement shall be deemed duly given when delivered personally, sent electronically by email, sent by facsimile with receipt acknowledged, mailed by prepaid registered mail, or certified mail, return receipt requested, or delivered by a recognized commercial carrier addressed to the address last designated on the MSA Order Form or such other address as designated in writing to the other party.

e. **Customer/Technical Support.** Citrix Online shall provide, at no additional charge to Customer, customer/technical support services as further described in Exhibit A attached hereto. Customer acknowledges it will be required, from time to time, to accept Service(s) updates at no additional charge to Customer, as part of Citrix Online's ongoing Service(s) enhancement and customer/technical support.

f. **High-Risk Use.** Customer hereby acknowledges that the Services are not designed or intended for access and/or use in or during high-risk activities including, but not limited to: medical procedures; on-line control of aircraft, air traffic, aircraft navigation or aircraft communications; or the design, construction, operation or maintenance of any nuclear facility. Citrix Online and MicroTech hereby expressly disclaims any express or implied warranty of fitness for such purposes.

g. No Waiver. The failure of either Customer or Citrix Online in any one or more instance(s) to insist upon strict performance of any of the terms of this Agreement will not be construed as a waiver or relinquishment of the right to assert or rely upon any such term(s) on any future occasion(s).

h. Severability. If any provision of this Agreement is declared by a court of competent jurisdiction to be invalid, illegal, or unenforceable, such provision shall be severed from this Agreement and the other provisions shall remain in full force and effect.

i. No Third Party Beneficiaries. No person or entity not a party to this Agreement will be deemed to be a third party beneficiary of this Agreement or any provision hereof.

j. Survival. The termination of this Agreement shall not relieve either party of any liability or obligation incurred prior to such termination. In addition, the provisions of Sections 2(d) (reverse engineering), 3 (Term and Termination), 5 (Confidential Information), 6 (Representations and Warranties), 7 (Indemnification), 8 (Limitation of Liability) and 9 (Additional Terms) shall survive any termination of this Agreement.

k. Entire Agreement. This Agreement, comprised of the MSA Order Form and these Terms and Conditions, including any exhibits attached hereto, sets forth the entire agreement and understanding of the parties relating to the subject matter hereof and supersedes all prior and contemporaneous oral and written agreements and understandings with respect to the same. No waiver or amendment of any term or condition of this Agreement shall be valid or binding on either party unless agreed to in writing by both parties. In the event Customer issues any documentation pursuant to Section 2(f), the same shall be subject to and a part of this Agreement, and any contradictory terms or conditions therein shall have no force or effect.

l. Captions and Headings. Captions and headings are used herein for convenience only, are not a part of this

Agreement, and shall not be used in interpreting or construing this Agreement.

m. Counterparts. This Agreement may be executed in one or more counterparts and by facsimile signature, each of which shall be deemed an original but all of which, taken together, shall constitute one and the same instrument.