MISSION SUPPORT AND TEST SERVICES, LLC

SUBCONTRACT

EXHIBIT F

SECURITY REQUIREMENTS

TABLE OF CONTENTS

NO.	TITLE	PAGE
F-1	Security Requirements	2
F-2	Security Requirements – Prohibited Articles Policy	4
F-3	Security Requirements – Controlled Articles Policy	7

EXHIBIT F

F-1 SECURITY REQUIREMENTS

1 Security Requirements (Basic Access)

1.1 The work site is located at the Nevada National Security Site (NNSS) and/or North Las Vegas Facility (NLVF). These locations are under the oversight of the Department of Energy (DOE) National Nuclear Security Administration/Nevada Field Office (NNSA/NFO). Within each location, several security areas exist with additional requirements. The CONTRACTOR will convey these requirements to the SUBCONTRACTOR, as applicable, and the SUBCONTRACTOR is responsible to adhere to those requirements.

1.2 SUBCONTRACTOR personnel requiring access to NNSA/NFO property must be a United States (U.S.) citizen, in the final decree, and at least 18 years of age.

SUBCONTRACTOR personnel will be required to obtain security badges upon entry to the NNSS and/or NLVF. Badges will be issued at no charge to the SUBCONTRACTOR.

SUBCONTRACTORs must have proper photographic identification (ID). Per NNSA guidance regarding REAL ID Act of 2005, a secondary form of photographic ID will be required for access/badging for personnel presenting noncompliant driver's licenses. Acceptable secondary forms of photographic ID include:

- U.S. Passport/U.S. Passport Card
- U.S. Customs and Border Protection trusted traveler card
- U.S. military ID card/U.S. military dependent ID card
- Department of Homeland Security-designated Enhanced Driver's License
- Native American tribal photo ID
- HSPD-12 Personal Identity Verification (PIV) card from any government agency (for identification only)
- Transportation Worker Identification Credential (TWIC)

1.2.1 SUBCONTRACTORs declaring U.S. citizenship that were born abroad must show documentation as proof of U.S. citizenship for access.

1.3 SUBCONTRACTOR personnel **working over 30 days** will be required to complete the initial security and Counterintelligence briefing. These personnel will be issued photo security badges after citizenship verification.

1.3.1 The SUBCONTRACTOR must furnish the CONTRACTOR the following information, for personnel working on site, four working days prior to commencing work:

- Full Name, including full middle name (as it appears on driver's license)
- Social Security Number
- Date of Birth and Place of Birth
- Citizenship **(must be U.S. citizen)**

1.3.2 Acceptable forms of proof of citizenship include:

- U.S.-issued passports
- Original birth certificates with a raised state seal (or a certified copy)
- State Department form for U.S. citizens born on military bases
- Original naturalization papers

Individuals who are resident aliens with green cards are NOT U.S. citizens and must be processed as a non-U.S. citizen.

1.4 Access to CONTRACTOR facilities or information by non-U.S. citizens, must be coordinated 45 days in advance with the CONTRACTOR security group.

1.5 If the SUBCONTRACTOR is required to take CONTRACTOR information to an offsite location, the information MUST NOT contain classified information. The SUBCONTRACTOR must ensure that the information is not accessed by any employee or person that is NOT a U.S. citizen, without prior approval.

1.6 Attached to this exhibit is the Prohibited Articles and Controlled Articles Policies. SUBCONTRACTORs must comply with the entire policy. Violating this policy may result in the SUBCONTRACTOR being permanently denied access to CONTRACTOR facilities.

1.7 SUBCONTRACTORs are not permitted access to security areas except for approved work-related activities.

1.8 SUBCONTRACTOR must comply with the CONTRACTOR and federal traffic regulations while on CONTRACTOR or federal roadways. It will be the responsibility of the SUBCONTRACTOR to familiarize itself and its personnel with the traffic and safety requirements that have been provided by the CONTRACTOR.

1.9 SUBCONTRACTOR vehicles will be restricted to CONTRACTOR established routes or as noted on the subcontract documents. SUBCONTRACTOR vehicles and/or hand-carried items are subject to search on NNSA/NFO property.

1.10 SUBCONTRACTOR-owned property shall be segregated from government property. SUBCONTRACTOR-owned property must be clearly marked or otherwise identified. The markings shall be securely affixed to the property, legible, and conspicuous.

Recommend the SUBCONTRACTOR make an inventory of their company property. Upon exit from the work site, SUBCONTRACTOR shall attach the inventory list to the Property Removal Authorization Form that has been provided by the CONTRACTOR.

F-2 SECURITY REQUIREMENTS – PROHIBITED ARTICLES POLICY

2 Prohibited Articles

Introducing a prohibited article onto NNSA/NFO property is a reportable security incident and may be subject to disciplinary and/or legal action.

Prohibited articles are restricted from introduction onto NNSA/NFO property. As there may be several variations or types of these prohibited articles, this list is not all-inclusive. Any item that may be questionable or in most cases a personal/private item, must be coordinated with MSTS Security Planning and Operations for clarification or approval prior to introduction.

ARTICLE	EXCEPTION
Firearms, projectile weapons, electric weapons, replica weapons, and ammunition	2.1.1
Destructive devices, explosives, or combustible chemical compounds and mixtures	2.1.2
Dangerous weapons	2.1.3
Alcoholic beverages	2.1.4
Controlled substances (e.g., illegal drugs, associated paraphernalia)	2.1.5
Disabling chemical	2.1.6
Optical devices	2.1.7
Global Positioning System (GPS)	2.1.8
Animals	2.1.9
Privately owned Unmanned Aerial Vehicle (e.g., unmanned aircraft, remotely piloted)	N/A
Items prohibited by local, state, federal law	N/A

EXHIBIT F

2.1 Applicable Exceptions

Other approved exceptions are detailed in the *Nevada Enterprise Prohibited and Controlled Articles Policy* available to the CONTRACTOR. Below are excerpts of exceptions applicable to this SUBCONTRACTOR solicitation.

2.1.1 Firearms, Projectile Weapons, Electric Weapons, Replica Weapons, and Ammunition

Should these items be required for work by the SUBCONTRACTOR, the CONTRACTOR office/individual responsible for the SUBCONTRACTOR must coordinate with MSTS Security Planning and Operations prior to introduction onto NNSA/NFO property.

2.1.2 Destructive Devices, Explosives, or Combustible Chemical Compounds and Mixtures

Government owned (owned by the United States and under the custody and control of a federal department or agency) destructive devices, explosives, or combustible chemical compound and mixtures are authorized on NNSA/NFO property in order to perform official duties, properly approved work, approved project activities, or approved training.

Road flares (e.g., vehicle-related safety equipment) are authorized only in a Property Protection Area (PPA).

2.1.3 Dangerous Weapons

A “dangerous weapon” is an implement, device, instrument, material, animate or inanimate meant to be used for or readily capable of causing death/serious bodily injury. Personally owned weapons, bladed/edged instrument, pick-like tool, club-like/striking device (including sporting equipment), or electric weapons (stun-gun, prod) are unauthorized.

A personally owned pocket-knife type/folding instrument with a blade of <u>less than 2.5 inches</u> in length is allowable.

This requirement does not prohibit employees from government owned/procured instruments for work/tools-of-the-trade (e.g., for the preparation/consumption of food, construction, or maintenance) or government owned/procured items as part of required/assigned duty equipment of law enforcement or uniformed security personnel. This includes government owned/procured items of approved project activities.

2.1.4 Alcoholic Beverages

MSTS-procured alcohol to be sold at the NNSS Mercury Cafeteria/Steak House, as part of an approved event, is authorized for consumption at that location.

Consumption of alcohol on NNSA/NFO property is prohibited unless approved by the NNSA/NFO Officially Designated Federal Security Authority. This prohibition includes NNSS official housing quarters and affiliated spaces.

2.1.5 Controlled Substances

Legally prescribed, federally recognized medications and delivery paraphernalia in the possession of or under the control of the individual who holds the prescription are authorized. Other fitness for duty restrictions on use, access, or duty limitations may apply.

2.1.6 Disabling Chemical

A disabling chemical is a substance that is designed or intended to temporarily incapacitate or disorientate a person, either physically or mentally (e.g., pepper spray).

2.1.7 Optical Devices

Government owned or government vendor/subcontractor optical devices (e.g., binoculars, monocular, telescopes) are authorized when used to perform approved work or activities.

Personally owned optical devices are authorized for only introduction. They must not be used and must be stored in a privately-owned vehicle.

2.1.8 Global Positioning Systems

Government owned or government vendor/subcontractor GPS specific/stand-alone hand-held devices are authorized when used to perform approved work or activities.

Personally owned GPS specific/stand-alone hand-held devices are authorized for only introduction into the PPA. They must not be used and must be stored in a privately-owned vehicle.

2.1.9 Animals

Service Animal: A service animal is defined by the Americans with Disabilities Act as a dog (canine) that is individually trained to do work or perform tasks for people with disabilities. Service animals may be introduced into areas that generally serve the public or where the public is allowed to go. Emotional support animals, comfort animals, therapy animals, and pets are not service animals.

The CONTRACTOR office/individual responsible for the SUBCONTRACTOR must coordinate with MSTS Security Planning and Operations/Facility Security Officer (FSO) prior to a service animal being on NNSA/NFO property. Additional restrictions may apply.

F-3 SECURITY REQUIREMENTS – CONTROLLED ARTICLES POLICY

3 Controlled Articles

Introducing unauthorized controlled articles into security areas is a reportable security incident and may be subject to disciplinary and/or legal action.

Controlled articles are devices that may be conditionally introduced into NNSA/NFO locations. Conditions are determined by MSTS Cyber Security and vary depending on device attributes and location use. The overall intent of the policy is to ensure the protection of security assets while enabling use of operational or business beneficial devices.

DOE/NNSA Managed refers to devices that have been procured, cataloged, and/or controlled by either the NNSA/NFO, NNSA/NFO contractors, or Nevada based Nuclear Weapons Laboratories.

Devices owned by subcontractors, other companies, or Other Government Agencies performing work or participating in activities with the NNSA/NFO may be afforded allowances similar to a DOE/NNSA Managed device. Devices must be submitted for MSTS Cyber Security review and approval, additional conditions/restrictions may be applied. Otherwise, these devices will be considered as a personal device.

For clarification regarding controlled article requirements or device review and approvals, contact MSTS Cyber Security (CyberSecurity@nv.doe.gov).

EXHIBIT F

3.1 Electronic Device

ELECTRONIC DEVICE Property Protection Area (PPA)	
CONDITION	
PPA	**Not authorized to connect to DOE/NNSA managed equipment and/or network resources.** Exceptions: - Cellular/Smart Phone/Tablet (DOE/NNSA Managed) - Computers/Laptop (DOE/NNSA Managed)
	Use of wireless hotspots is not authorized.
	Use of audio, photography, and video functions <u>for the purpose of recording</u> are not authorized. Exceptions: - Cameras (DOE/NNSA Managed, Derivative Classifier/Reviewing Official [DC/RO] review required) - Cellular/Smart Phone/Tablet (DOE/NNSA Managed, DC/RO review required) - QR Code (Government or company produced QR Code captured by a DOE/NNSA Managed device) - Vehicle Cameras/Vehicle Event Recorders
	Confirm devices are not manufactured by a federally restricted company.
	If unsure that a device can be introduced/used, contact M&O Cyber Security.

REQUIRED ELECTRONIC DEVICE REVIEW and APPROVAL Certain electronic devices must be reviewed and approved by M&O Cyber Security. Approvals may be accompanied with additional restrictions. Requests must be submitted to M&O Cyber Security (CyberSecurity@nv.doe.gov) for the following.	
REVIEW REQUIRED	
PPA **LA** **VAULT** **VTR** **PA** **MAA**	**Devices to be introduced and/or used in security areas/storage (LA or higher).**
	Devices to be connected to DOE/NNSA Managed equipment and/or network resources.
	Procurement of electronic devices.
	Devices that process, store, or collect data. *
	Devices with Global Positioning System / Navigation functions (LA or higher). **
	Any device that does not meet requirements of this plan or any device that may be questionable, undetermined, or needing clarification.
	MEDICAL DEVICE (Electronic and/or Wireless Capability)
	Must be Medical Electronic Device Security and Approval Framework (MEDSAFe) approved. **Additional M&O Cyber Security approval may be required for PA and MAA introduction.**

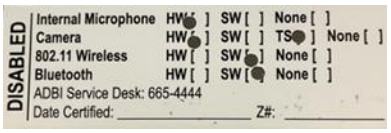
* Government owned or Government vendor/subcontractor vehicle cameras and vehicle event recorders are authorized in Limited Areas or higher security locations. The sponsor/escort is responsible to ensure recording capability of vehicle cameras are disabled or shrouded.

** Government owned or Government vendor/subcontractor vehicle equipped GPS / navigation functions are authorized in Limited Areas or higher security location (e.g., fleet trackers).

LA = Limited Area; VTR = Vault-Type Room; PA = Protected Area; MAA = Material Access Area

EXHIBIT F

3.2 Authorized Laptops / Desktops (Stand-Alone)

Laptops/Desktops (Stand-Alone) authorized into a Limited Area or higher security location require built-in wireless, microphone, and camera to be disabled in the basic input/output system (BIOS), unless an exemption is approved by M&O Cyber Security.	
CONDITION	
LA	**Laptops / Desktops (Stand-Alone) authorized into LAs must be identified by the following Cyber Security labels:**
	M&O Cyber Security 
	Los Alamos National Laboratory Cyber Security 
	Lawrence Livermore National Laboratory Cyber Security  
VAULT **VTR** **PA** **MAA**	**Laptops / Desktops (Stand-Alone) must meet LA conditions.**
	Laptops / Desktops (Stand-Alone) must receive specific approval from M&O Cyber Security.
	M&O Cyber Security approval documentation must be provided upon request.

3.3 Authorized Recording

DOE/NNSA Managed devices must be used to conduct authorized recordings (audio, photographic, and video) unless an exemption is approved by M&O Cyber Security.	
CONDITION	
PPA	**DC/RO review/determination completed prior to distribution or system uploading/downloading.**
LA **VAULT** **VTR** **PA** **MAA**	**M&O Cyber Security recording device approval.**
	DC/RO review/determination completed prior to distribution or system uploading/downloading.
	Device and media must be protected at the highest level/most restrictive category for which the area is authorized, until reviewed by a DC/RO.