



Nevada Enterprise Prohibited and Controlled Articles Policy

SP-2300.001 Section 8.2 / Annex 1

Revision 4 (Excerpt)

Supersedes: *Nevada Enterprise Prohibited and Controlled Articles Policy*, Revision 3
Prepared by: Mission Support and Test Services, Security Planning and Operations

TABLE OF CONTENTS

1	PURPOSE	3
2	EXCERPT	4
8.2	Prohibited and Controlled Articles	4
8.2.1	Prohibited Articles.....	4
8.2.2	Prohibited Article Exceptions	5
8.2.3	Incidents Involving Prohibited Articles.....	8
8.2.4	Controlled Articles	8
8.2.5	Request to Introduce Unapproved Controlled Articles	9
8.2.6	Medical Devices (Electronic)	9
8.2.7	General Access Area Prohibited and Controlled Articles	10
	ANNEX 1: Controlled Articles.....	11
1	Controlled Articles	11
1.1	Electronic Device.....	12
1.2	Authorized Laptops / Desktops (Stand-Alone)	13
1.3	Authorized Recording	13

1 PURPOSE

This document is a collection of references taken from *SP-2300.001, Nevada Enterprise Site Security Plan, Revision 4*. Requirement information is extracted from the primary security plan and combined into this more accessible guidance document. The information within retains the primary security plan identifiers for reference purposes. This document is unclassified and approved for public release.

2 EXCERPT

8.2 Prohibited and Controlled Articles

The *Prohibited and Controlled Articles Policy* is issued under the authority of the Management and Operating (M&O) (contractor) and approval by the Officially Designated Federal Security Authority (ODFSA) (federal). The requirements are to be implemented consistently and equally.

Personnel are restricted from introducing prohibited and controlled articles onto Department of Energy (DOE) National Nuclear Security Administration/Nevada Field Office (NNSA/NFO) property without authorization. Personnel who observe the introduction or presence of prohibited and controlled articles will contact the Incident of Security Concern (IOSC) Hotline or M&O Security Planning and Operations/Facility Security Officer (Outlying Areas).

Personnel must conduct appropriate security area entry and exit inspections (where applicable) of other personnel, vehicles, packages, and hand-carried articles. Personnel will report on the discovery of unauthorized prohibited and controlled articles.

M&O Security Planning and Operations has the primary responsibility for maintaining the prohibited articles requirements and coordinating ODFSA authorization (via M&O Security and Emergency Services [SES] Senior Director/designee) for non-compliant prohibited articles and controlled articles.

M&O Cyber Security has the primary responsibility of controlled articles requirements.

8.2.1 Prohibited Articles

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 M&O Security Planning and Operations for clarification or approval prior to introduction.

Table 18: Prohibited Articles

ARTICLE	EXCEPTION
Firearms, projectile weapons, electric weapons, replica weapons, and ammunition	8.2.2.1
Destructive devices, explosives, or combustible chemical compounds and mixtures	8.2.2.2
Dangerous weapons	8.2.2.3
Alcoholic beverages	8.2.2.4
Controlled substances (e.g., illegal drugs, associated paraphernalia)	8.2.2.5
Disabling chemical	8.2.2.6
Optical devices	8.2.2.7
Global Positioning System (GPS)	8.2.2.8
Animals	8.2.2.9
Privately owned Unmanned Aerial Vehicle (e.g., unmanned aircraft, remotely piloted)	N/A
Items prohibited by local, state, federal law	N/A

8.2.2 Prohibited Article Exceptions

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

8.2.2.1.1 Allowed in the lawful/authorized performance of official duties and are directly affiliated with/employed by the following:

- M&O Protective Force and Protective Force Training (including other NNSA-complex protective force personnel attending training or supporting an event on site).
- M&O Performance Testing and Emergency Planning.
NOTE: Inert and replica firearms/weapons only, for exercise/training purposes).
- Office of Secure Transportation.
- Local Law Enforcement Agency (LLEA) assigned to conduct law enforcement duties at the Nevada National Security Site (NNSS) or LLEA responding to incidents, alarms, or emergencies on NNSA/NFO property.

8.2.2.1.2 Allowed in the lawful/authorized performance of duties by an officer, agent, or employee of the United States, State, or subdivision thereof, and are directly affiliated with/employed by the following:

- Department of War.
- Federal Agents (Agencies not listed are reviewed on a case-by-case basis).
 - Federal Bureau of Investigation.
 - Marshal Service.
 - Central Intelligence Agency.
 - Department of Homeland Security.
 - Department of State Diplomatic Security Service.
 - Secret Service.
- Federal or State Protective Detail.
- Law enforcement agencies not affiliated with NNSA/NFO locations are reviewed on a case-by-case basis.

8.2.2.1.2.1 The Host/Sponsor must coordinate with M&O Security Planning and Operations prior to entry of armed personnel. Notification will include name, organization, and visit locations of armed personnel. M&O Security Planning and Operations will provide follow-on notification to the NNSA/NFO Assistant Manager for Safeguards and Security (AMSS).

8.2.2.1.2.2 The NNSA/NFO AMSS must provide PA and MAA access authorization for armed personnel that are unaffiliated with the NNSA.

8.2.2.1.3 Commercial armored transportation services on official business are allowed to maintain work-assigned weapons and ammunition on NNSA/NFO property. Access is secured through M&O Personnel Security and coordinated with M&O Security Planning and Operations. Upon arrival, the commercial armored transportation service courier must present badges and credentials (if applicable) to the Protective Force at the access point. Personnel must declare their armed status and official business and provide the name of the facility/individual with which they have business. The Protective Force must verify personnel with the information provided by M&O Security Planning and Operations.

- 8.2.2.1.4 Long-haul truck drivers/commercial delivery drivers are authorized to temporarily store privately-owned firearms/ammunition in a shipping container (also may be referred to as a CONEX) located at the NNSS (General Access Area) parking area/truck depot lot.
- Drivers requesting to temporarily store firearms/ammunition will be directed to the container. Notify M&O Security Planning and Operations or Protective Force Headquarters (Non-Working Hours). The Protective Force will be notified of storage requests and proceed to the container.
 - Drivers must retrieve privately-owned firearms by the close of business. The Protective Force will perform an end-of-day check of the container. Firearms and ammunition left beyond the end of normal working hours will be transferred to the Nye County Sheriff's Office.
 - This temporary storage service is not available to M&O, Nuclear Weapons Laboratories, or other DOE and/or contractor/subcontractor employees.
 - The M&O has no direct responsibility for privately-owned firearms/ammunition. Both the compound gate and container will be secured when storing a privately-owned firearm.
 - At no time will any DOE asset be stored in the container.
 - The temporary stored private property will be secured by a non-security level lock; the key will be retained by the Protective Force.
- 8.2.2.1.5 Authorized vendor/commercial delivery services may transport commercially packaged ammunition to/from the NNSS Mercury Warehouse. Onsite hazardous material and/or explosive transportation and notification requirements apply.
- 8.2.2.2 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).
- 8.2.2.3 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 instruments, pick-like tools, club-like/striking devices, or electric weapons (stun-gun, prod) are unauthorized.
- A personally owned pocket-knife type/folding instrument with a blade of less than 2.5 inches 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 federal agents/law enforcement, uniformed Protective Force, or LLEAs. This includes government owned/procured items of approved project activities.
- 8.2.2.4 Alcoholic Beverages
- M&O-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.
- Sealed containers of alcohol are authorized if part of an on-site gift exchange.

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

8.2.2.5 Controlled Substances

Controlled substances and delivery paraphernalia in the possession of/under the control of on-duty Fire and Rescue/Emergency, Occupational Medicine, federal agents/law enforcement, or LLEA personnel are authorized.

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 and Human Reliability Program (HRP) restrictions on use, access, or duty limitations may apply.

8.2.2.6 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).

This requirement does not prohibit items as part of required/assigned duty equipment of federal agents/law enforcement, uniformed Protective Force, or LLEA personnel.

8.2.2.7 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 into the PPA. They must not be used and must be stored in a privately-owned vehicle.

8.2.2.8 Global Positioning Systems

Government owned or government vendor/subcontractor global positioning system (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.

The use of GPS as a function will be controlled, reference *Controlled Articles*.

8.2.2.9 Animals

- 8.2.2.9.1 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 employee, visitor, and/or host must coordinate with M&O Security Planning and Operations/Facility Security Officer prior to a service animal being on NNSA/NFO property.

- 8.2.2.9.1.1 Introduction of service animals into a PPA is allowed, unless security or safety reasons exist, as determined by M&O Security Planning and Operations/Facility Security Officer.

- 8.2.2.9.1.2 Introduction of service animals into a security area or secure storage area will be reviewed by M&O Security Planning and Operations/Facility Security Officer, prior to introduction of the service animal. If the review determines an issue may exist, additional review/approval from M&O SES security management may be required.

- 8.2.2.9.1.3 Introduction of service animals into a Protected Area (PA)/Material Access Area (MAA) requires an appropriate security/safety review and approval by the ODFSA.
- 8.2.2.9.1.4 Introduction of service animals into a Sensitive Compartmented Information Facility (SCIF) or Special Access Program Facilities (SAPF) requires coordination and authorization from the Field Intelligence Element, Director.
- 8.2.2.9.2 Working Canine: A working canine is defined as a canine that is trained and certified for explosives detection, contraband detection, drug detection, human detection, and/or other law enforcement, military, or rescue search functions. Law enforcement, Fire and Rescue/Emergency, or Other Government Agency personnel in the lawful/authorized performance of official duties, are authorized to have accompanying working canines. Equipment associated with the training, care, and protection of a working canine is authorized.
- 8.2.2.9.3 Working Animal (Non-Canine): A working animal (other than a working canine) owned and used by a law enforcement agency, Fire and Rescue/Emergency organization, or Other Government Agency must be coordinated with M&O Security Planning and Operations prior to introduction onto NNSA/NFO property. Review/approval from M&O SES security management may be required.
- 8.2.2.10 Exceptions not identified above can be submitted to the ODFSA through the M&O SES Senior Director. The requesting organization will provide the M&O SES Senior Director with justification and supporting information for the request.

8.2.3 Incidents Involving Prohibited Articles

Introducing a prohibited article is a reportable security incident. Personnel who introduce prohibited articles may be subject to disciplinary and legal action. Prohibited articles may be confiscated by the Protective Force, security personnel, or LLEAs.

- 8.2.3.1 Discovery of a prohibited article that violates local, state, or federal laws, will prompt additional action and LLEA must be contacted.
- 8.2.3.2 Prohibited article requirements do not apply to shared public parking lots of leased facilities.

8.2.4 Controlled Articles

Controlled articles are items, primarily electronic and/or technology devices, that may be introduced into security areas, after certain conditions have been met. These conditions vary depending on the attributes of the controlled article and the security area. The overall intent of the controlled article policy is to ensure the protection of security assets while enabling use of operational or business beneficial items. Annex 1, Controlled Articles provide basic allowances for use, determined by M&O Cyber Security. Items, or an allowance not identified, must be submitted to M&O Cyber Security for review and approval. Some items may additionally need to be submitted for review, as a condition for use.

8.2.4.1 Authorized Recording

NNSA managed devices (government owned/controlled) must be used to conduct recordings (audio, photographic, and video) unless an exception is approved by M&O Cyber Security.

- Recording device use in a Limited Area (LA) or higher security area must be authorized by M&O Cyber Security.
- Recording of video conferencing sessions must be authorized by M&O Cyber Security.

- A Derivative Classifier/Reviewing Official (DC/RO) review and determination must be completed prior to distribution or system uploading/downloading of the recording (audio, photographic, and video).
- The recording 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.
- Recording device M&O Cyber Security approval document must be presented upon request.

8.2.5 Request to Introduce Unapproved Controlled Articles

Items that do not meet the requirements for introduction or use must be reviewed and approved by M&O Cyber Security. M&O Technical Analysis may be involved when the review is determined to require ODFSA approval. Initiate reviews through M&O Cyber Security.

8.2.5.1 Requestors must provide the following initial information:

- Who is making the request and what is requested for introduction.
- Where the article is intended to be used and how the article is being used.
- When the desired date of introduction (and duration) will occur.
- Why the article is being requested along with its necessity for use.

8.2.5.1.1 The requestor must provide documentation to support the review:

- Current device/equipment specification sheets.
- Device/equipment instruction manuals.
- Any other documentation to aid in the cyber/technical review.

8.2.5.2 M&O Cyber Security Review

8.2.5.2.1 A review of the device information provided and/or direct discussions with item manufacturer will occur. A physical examination of the item may also be required.

8.2.5.2.2 M&O Cyber Security will review the area of intended use to determine if the device can be introduced without introducing a technical security hazard.

8.2.5.2.3 M&O Cyber Security may determine that a follow-on evaluation by the Technical Surveillance Countermeasures (TSCM) team is required. TSCM will provide a report (In favor of introduction/not in favor of introduction).

8.2.5.2.4 In addition, countermeasure considerations and residual risk input by the NNSA Certified TEMPEST Technical Authority (CTTA) may accompany the recommendation.

8.2.5.3 M&O Technical Analysis

8.2.5.3.1 Should reviews require ODFSA approval, M&O Technical Analysis will review impacts and determine the impact to risk. Analysis will incorporate their item review and input.

8.2.5.3.2 An Unanalyzed Security Condition (USC) will be initiated to define impacts to risk for situations not analyzed. The completed USC is submitted to the ODFSA for notification, concurrence, or approval.

8.2.6 Medical Devices (Electronic)

Medical devices that are electronic and/or use any type of wireless capability must be reviewed and approved through the NA-70 Medical Electronic Device Security and Approval Framework (MEDSAFE) process prior to their introduction into a security area.

8.2.6.1 Medical Device (Electronic) Approval Process (LA or higher security area)

- Request submission through MEDSAFe (medsafe.doe.gov).
- MEDSAFe distributes the request to M&O Occupational Medicine for review of the legitimate medical condition and medical device justification.
- MEDSAFe distributes the request to M&O Cyber Security for technical assessment of the device.
- An approval or denial formulated by the collaborative review of M&O Occupational Medicine and M&O Cyber Security, is communicated through MEDSAFe to the requestor.

8.2.6.2 Medical Device (Electronic) Approval Process (PA and MAA)

- Obtain MEDSAFe approval for the requested device.
- Contact M&O Cyber Security to request device introduction into a PA and MAA. If approved, the requestor will receive documentation specific to a PA and MAA.

8.2.6.3 Approval documents must be presented upon request prior to accessing a security location.

8.2.6.4 For information on the MEDSAFe process, contact M&O Occupational Medicine and M&O Cyber Security.

8.2.6.5 M&O SES Senior Director Limited Authority (Unreviewed Medical Devices)

Should the ODFSA not be available to approve the introduction of an unreviewed medical device into a security area/storage location (LA or higher), the M&O SES Senior Director has authority to allow the introduction of the medical device for the following circumstances:

- Medical and/or fire emergencies.
- Personnel critical in addressing emergency situations.
- Events where access is determined to be expeditiously necessary.

8.2.6.5.1 Authorizations will be accompanied by subsequent ODFSA notification. A notification email will be sent to the ODFSA and M&O Cyber Security Manager with the following:

- Name of personnel with medical device.
- Medical device name and model.
- Date and time.
- Reason.

8.2.7 General Access Area Prohibited and Controlled Articles

8.2.7.1 Prohibited articles are restricted from introduction.

8.2.7.2 Controlled Articles

8.2.7.2.1 Employees/contractors/visitors will comply with PPA controlled articles requirements while in the General Access Area or as coordinated with the Operations Command Center (OCC) or M&O Security Planning and Operations. Devices may be confiscated and final disposition is determined by the IOSC Inquiry Official.

8.2.7.2.2 Unauthorized personnel (e.g., Trespasser) device confiscation/searching will be determined by LLEA or federal law enforcement.

ANNEX 1: Controlled Articles

1 Controlled Articles

Controlled articles are devices that may be conditionally introduced into U.S. Department of Energy (DOE), National Nuclear Security Administration Nevada Field Office (NNSA/NFO) locations. Conditions are determined by Management and Operations (M&O) 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.

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. The NNSA Office of Secure Transportation (in the performance of official duties) is exempt from device review and approval.

Devices owned by subcontractors, other companies, or Other Government Agencies performing work or participating in activities on NNSA/NFO property may be afforded allowances similar to a DOE/NNSA Managed device. Devices must be submitted for M&O 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 M&O Cyber Security (CyberSecurity@nv.doe.gov).

1.1 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, photographic, 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	

1.2 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.

1.3 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.