



Nevada Enterprise Prohibited and Controlled Articles Policy

SP-2300.001 8.2 / Annex 1 (Revision 3 Excerpt)

Supersedes: *Nevada Enterprise Prohibited and Controlled Articles Policy*, Revision 2
Prepared by: Mission Support and Test Services, Security Planning and Operations

8.2 Prohibited and Controlled Articles

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 across organizations, facilities, areas, and operations. This consistent implementation requires organizations to follow these requirements without the option of imposing more restrictive requirements on facilities, areas, or operations.

Personnel are restricted from introducing prohibited/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/controlled articles will contact the Operations Command Center (OCC) or M&O Security Planning and Operations/Facility Security Officer (FSO) (Outlying Areas).

The Protective Force (PF) must conduct appropriate entry and exit inspections (where applicable) of personnel, vehicles, packages, and hand-carried articles. The PF will follow order requirements upon discovery of unauthorized prohibited/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. Primary guidance regarding prohibited articles will be per DOE O 473.1A, *Physical Protection Program* and the referenced federal regulations and codes within. 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 onto NNSA/NFO property.

Table 14: Prohibited Articles

ARTICLE	EXCEPTION
Firearms, projectile weapons, electric weapons, replica weapons, and ammunition	Exception (8.2.1.1.1)
Destructive devices, explosives, or combustible chemical compounds and mixtures	Exception (8.2.1.1.2)
Dangerous weapons	Exception (8.2.1.1.3)
Alcoholic beverages	Exception (8.2.1.1.4)
Controlled substances (e.g., illegal drugs, associated paraphernalia)	Exception (8.2.1.1.5)
Disabling chemical	Exception (8.2.1.1.6)
Optical devices	Exception (8.2.1.1.7)
Global positioning systems (GPS)	Exception (8.2.1.1.8)
Animals	Exception (8.2.1.1.9)
Privately owned Unmanned Aerial Vehicle (e.g., drones, unmanned aircraft, remotely piloted)	NO EXCEPTIONS
Items prohibited by local, state, federal law	NO EXCEPTIONS

8.2.1.1 Exceptions

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

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

- PF and PF Training/Performance Testing (including other NNSA contractor PF personnel attending training or supporting an event onsite).
- Office of Secure Transportation.

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

- Department of Defense. (Host/Sponsor must contact M&O Security Planning and Operations prior to entry).
- Federal Agents (Host/Sponsor must contact M&O Security Planning and Operations prior to entry. Agencies not listed are reviewed by M&O Security Planning and Operations 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 Department of Defense Protective Detail. (Host/Sponsor must contact M&O Security Planning and Operations prior to entry).
- Local Law Enforcement Agency (LLEA) (Host/Sponsor must contact M&O Security Planning and Operations prior to entry, with the exception of LLEA assigned to conduct law enforcement duties at the Nevada National Security Site (NNSS) or LLEA responding to alarms or emergencies).

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

8.2.1.1.1.3 Commercial armored transportation services on official business are allowed to maintain work-assigned weapons and ammunition on NNSA/NFO property. The office/individual responsible for requesting these services must coordinate access with M&O Security Planning and Operations prior to entry. Upon arrival, the commercial armored transportation service driver must present badges and credentials (if applicable) to the PF at the access point. Personnel must declare their armed status and official business and provide the name of the office/individual with which they have business. PF must verify personnel with the information provided by M&O Security Planning and Operations.

8.2.1.1.1.4 At the NNSS, 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.

- When drivers request to temporarily store firearms/ammunition, they will be directed to the container. Notify M&O Security Planning and Operations or PF Headquarters (Non-Working Hours). PF will be notified of storage requests and proceed to the container.
- The M&O has no direct responsibility of privately-owned firearms/ammunition. Both the 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 temporarily stored private property will be secured by a non-security level lock, the key will be retained by the PF.
- Drivers must retrieve privately-owned firearms by the close of business. PF will perform an end of day check of the container. Firearms/ammunition left beyond the end of normal working hours will be transferred to Nye County Sheriff's Office.
- This service is not available to M&O, Nuclear Weapons Laboratory, or other DOE and/or contractor/subcontractor employees.

8.2.1.1.1.5 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.

8.2.1.1.2 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 NNSS/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).

8.2.1.1.3 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, 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 PF, or LLEAs. This includes government owned/procured items of approved project activities.

8.2.1.1.4 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 are authorized if part of an onsite gift exchange. Consumption of alcohol anywhere other than the cafeteria, is prohibited unless approved by the ODFSA. This prohibition includes NNSS official housing quarters and affiliated spaces.

8.2.1.1.5 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 restrictions on use, access, or duty limitations may apply.

8.2.1.1.6 Disabling Chemical

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

8.2.1.1.7 Optical Devices

Government owned optical devices (e.g., binoculars, monocular, telescopes) may be authorized for introduction into security areas, when used to perform properly 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.

8.2.1.1.8 Global Positioning Systems

Government owned or government vendor/subcontractor GPS/navigation equipped functions are authorized.

Personally owned GPS/navigation equipped functions are only authorized in PPAs unless approved otherwise by M&O Cyber Security.

8.2.1.1.9 Animals

Service Animal: A service animal is defined by the Americans with Disabilities Act (ADA) as a dog 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, and therapy dogs are not service animals.

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

- Introduction of service animals into a PPA is allowed, unless security or safety reasons exist, as determined by M&O Security Planning and Operations/FSO.
- Introduction of service animals into a security area or secure storage area (e.g., Limited Area or Vault-Type Room) will be reviewed by M&O Security Planning and Operations/FSO, 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.
- Introduction of service animals into a Protected Area (PA)/Material Access Area (MAA) requires an appropriate security and safety review and approval by the ODFSA.

Search Animal: A search animal is defined as an animal that is trained and certified for explosives, contraband, drug, or rescue search functions. Law enforcement personnel and Fire and Rescue/Emergency personnel, in the performance of official duties, are authorized

to have accompanying search animals. Equipment associated with the search animal is authorized.

- 8.2.1.1.10 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 a justification and supporting information for the request.

8.2.1.2 Incidents Involving Prohibited Articles

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

- 8.2.1.2.1 Discovery of a prohibited article that violates local, state, or federal laws, will prompt additional action and LLEA must be contacted.

- 8.2.1.2.2 Prohibited article requirements do not apply to shared public parking lots for NNSA/NFO leased facilities.

8.2.2 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.

- 8.2.2.1 The controlled article reference table is located in Annex 1, "Controlled Articles." The table provides basic allowances for use as determined by M&O Cyber Security. For clarification on controlled article requirements, contact M&O Cyber Security.

- 8.2.2.2 Items or an allowance not identified in the reference table must be submitted to M&O Cyber Security for review and approval. Some items identified in the table may additionally need to be submitted to Cyber Security as a condition for use.

8.2.3 Special Permits

8.2.3.1 General

- 8.2.3.1.1 Special Permits only apply to NNSA managed devices (Government owned/controlled). Personally owned recording devices are unauthorized for use.

- 8.2.3.1.2 Special Permits are issued to personnel requiring the use of NNSA managed devices (Government issued/controlled) within a Limited Area or higher security area/location. Personnel do not require a Special Permit for use of NNSA managed (Government owned/controlled) camera/video recorders and audio recording devices in PPAs.

- 8.2.3.1.3 Only the minimum number of permits needed to accomplish work will be approved. Special Permits authorize cleared personnel to possess and/or use camera/video recorders and audio recording devices in the performance of official duties.

- 8.2.3.1.4 Recording video conferencing session is not authorized without M&O Cyber Security approval.

- 8.2.3.1.5 NNSA managed devices (Government owned/controlled) specifically associated with the capture of scientific/informational data (e.g., oscilloscope, infrared, x-ray, optical data) in the performance of an authorized project/activity/work do not require a Special Permit.

NOTE: For the use of a NNSA managed (Government owned/controlled) stand-alone hand-held camera to photograph/video scientific/informational data displayed on another device, Special Permit requirements will apply.

8.2.3.2 Obtaining a Special Permit

8.2.3.2.1 Personnel must perform work necessitating an NFO-322, "NFO Special Permit."

8.2.3.2.2 Requests are submitted to/processed through M&O Security Planning and Operations or FSO. Requestors will follow the direction of M&O Security Planning and Operations/FSO to complete the requests.

NOTE: M&O Security Planning and Operations/FSOs may deny permit requests if other personnel in the requestors work organization hold an NFO-322.

8.2.3.2.3 Personnel will be notified by M&O Security Planning and Operations upon approval and notified of location for pick-up. Personnel must surrender the expired NFO-322.

8.2.4 Request to Introduce Unapproved Controlled Articles

Items/devices not captured in Annex 1 or not approved by the conditions of the reference tables must be reviewed and approved by M&O Cyber Security prior to introduction. In some instances, M&O Technical Analysis will be involved when the resulting cyber review is determined to require ODFSA concurrence/approval. The review process may be very lengthy; therefore, it is imperative items are submitted well in advance.

8.2.4.1 Personnel may initiate reviews through M&O Cyber Security.

8.2.4.1.1 Requestor must provide the following initial information:

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

8.2.4.1.2 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.

8.2.4.2 M&O Cyber Security Review

8.2.4.2.1 Collected information will be submitted to Cyber Security. A review of provided information and/or direct discussions with item manufacturer will occur.

8.2.4.2.2 Cyber Security will review the area of intended use, (e.g., location/vicinity of classified processing), to determine if the article can be introduced without introducing a technical security hazard.

8.2.4.2.3 Cyber Security may require a physical examination of the item.

- 8.2.4.2.4 Cyber Security may determine that a follow on evaluation by the Technical Surveillance Countermeasures (TSCM) team is required. TSCM will provide the results (In favor of introduction/not in favor of introduction) to the NNSA/NFO.
- 8.2.4.2.5 In addition, countermeasure considerations and residual risk input by the NNSA Certified TEMPEST Technical Authority (CTTA) may accompany the recommendation.
- 8.2.4.3 M&O Technical Analysis
- 8.2.4.3.1 Should M&O Cyber Security reviews require ODFSA approval, M&O Technical Analysis will review impacts and determine the impact to risk. Analysis will incorporate Cyber Security item review and input.
- 8.2.4.3.2 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.

8.2.5 Medical Devices (Electronic)

- 8.2.5.1 Medical devices that are electronic and/or use any type of wireless capability must be reviewed and approved by M&O Cyber Security prior to their introduction into a security area (Limited Area or higher security area). Common devices include, but not limited to, hearing devices, glucose monitors, or heart related devices.
- To initiate requests, provide basic request information to M&O Cyber Security (CyberSecurity@nv.doe.gov). The basic information should be limited to user/requestor name, device model, and location of requested use. Should additional information be needed, an M&O Cyber Security representative will reach out to the user/requestor. The review process may be lengthy, a 30-day lead time is requested to meet request dates. After review, M&O Cyber Security will issue an approval document with allowances and restrictions.
- 8.2.5.2 M&O SES Senior Director Limited Authority (Unreviewed Medical Devices)
- Should the ODFSA not be immediately available to approve the introduction of an unreviewed medical device into a security area (Limited Area or higher security area), the M&O SES Senior Director has authority to allow the medical device in the security area for the following circumstances:
- Medical and/or fire emergencies.
 - Personnel critical to addressing emergency situations.
 - Events where access is determined to be expeditiously necessary.
- 8.2.5.2.1 Authorizations will be accompanied by subsequent notification to the ODFSA. In addition, a notification email to the ODFSA and M&O Cyber Security Manager with the following information will be sent:
- Name of personnel with medical device.
 - Medical device name and model.
 - Date and time.
 - Reason.

8.2.6 General Access Area Prohibited and Controlled Articles

8.2.6.1 Prohibited Articles are restricted from introduction.

8.2.6.2 Controlled Articles

8.2.6.2.1 Nevada Enterprise employees/contractors/visitors will comply with Annex 1, "Controlled Articles," Electronic Device PPA requirements while in the General Access Area or as coordinated with the OCC or M&O Security Planning and Operations. Devices may be confiscated by PF or FSOs and final disposition determined by the Incident of Security Concern (IOSC) Inquiry Official.

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

8.2.7 *This section is not applicable to this excerpt and is omitted.*

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 (OGA) 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 ONLY	Not authorized to connect to DOE/NNSA managed equipment and/or network resources. Exceptions: - Cellular/Smart Phone (DOE/NNSA Managed) - Tablet (DOE/NNSA Managed) - Computers/Laptop (DOE/NNSA Managed)
	Use of wireless hotspots are 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 (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 personal or independently procured devices are not manufactured by a federally restricted company (Huawei, ZTE, etc.) prior to introduction onto DOE/NNSA property.
	If unsure that a device can be introduced/used in a PPA, contact M&O Cyber Security.
<p>* Government owned or Government vendor/subcontractor vehicle cameras and vehicle event recorders are also authorized in Limited Areas or higher security location. However, the sponsor/escort is responsible to ensure recording capability of vehicle cameras are disabled or shrouded.</p> <p>DOE/NNSA = Department of Energy/National Nuclear Security Administration</p>	

REQUIRED ELECTRONIC DEVICE REVIEW and APPROVAL	
<p>Certain electronic devices must be reviewed by M&O Cyber Security for approval. Approvals may be accompanied with additional restrictions.</p> <p>Requests must be submitted to M&O Cyber Security (CyberSecurity@nv.doe.gov) for the following:</p>	
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.
	Medical devices (electronic and/or any type of wireless capability) (LA or higher). *
	Any device that does not meet requirements of this plan or any device that may be questionable, undetermined, or needing clarification.
<p>* A 30-day lead time is requested to meet request dates.</p> <p>LA = Limited Area; VTR = Vault-Type Room; PA/MAA = Protected Area/Material Access Area</p>	

1.2 Authorized Laptops

CONDITION	
LA	Laptops authorized into LAs must be identified by the following Cyber Security labels:
	<div>M&O Cyber Security</div> 
	<div>LANL Cyber Security</div> 
	<div>LLNL Cyber Security</div> 
VAULT	Laptops must meet LA conditions.
VTR	Laptops must receive specific approval by the respective Cyber Security group.
PA/MAA	Cyber Security approval documentation must be provided upon request.
LANL = Los Alamos National Laboratory; LLNL = Lawrence Livermore National Laboratory	

1.3 Authorized Recording

CONDITION	
PPA	DC/RO review/determination completed prior to distribution or system uploading/downloading.
LA VAULT VTR PA/MAA	NFO-322, "NFO Special Permit," is required prior to recording device use/introduction.
	M&O Cyber Security recording device approval.
	DC/RO review/determination completed prior to distribution or system uploading/downloading.
PA/MAA	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.